

From: **Andrew Kingman** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPHA Public Comment - Pindrop Security, Inc.
Date: 22.08.2022 23:36:23 (+02:00)
Attachments: Pindrop Security, Inc. - Comments on CCPA Regulations.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,
On behalf of Pindrop Security, Inc., please find attached comments regarding the CCPA draft regulations. We would welcome an opportunity to answer any questions the CPHA may have.

Respectfully submitted,
Andrew A. Kingman

Andrew Kingman

President



www.marinerstrategies.com





August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: Pindrop Comments on CCPA Regulations

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

Pindrop is at the forefront of innovation in the authentication and anti-fraud field, giving people seamless, safe ways to access the parts of life that are most important to them. In an environment where consumers are fighting every day for their privacy and online safety, Pindrop allows consumers to use their voices as a key to unlock their worlds. Using our proprietary technology, Pindrop partners with government stakeholders, financial institutions, telecommunication providers, and other technology companies to help keep consumers and the businesses used by those consumers safe from increasingly advanced identity theft threats and criminal actors.

These threats are not hypothetical, nor are they rare in number. As you well know, a data security incident represents an existential threat for businesses, and businesses in California, as well as other states, are required to take reasonable measures in order to protect their consumer, employee, and business data.

Pindrop solutions empower California consumers and the businesses they rely on for everyday life to help prevent fraud and authenticate and authorize those consumers using their voice. This represents a generational improvement over other systems, notably “knowledge-based authentication,” (KBA) which have sufficed in the past, but that are increasingly susceptible to fraudsters’ ability to navigate these question-and-answer authentication processes. In 2021, a Pindrop study demonstrated that in one case, fraudsters actually had a higher passage rate on KBA questions than customers.¹ Instead of filling in questions that can be easily guessed by criminals, Pindrop harnesses the power of an individual’s most human characteristic – their voice – and empowers that person to connect to what they need at any given moment, while safeguarding their privacy.

Additionally, as one-time password (OTP) authentication has become increasingly popular, fraudsters have mirrored the innovation by developing bots to intercept these passwords.² Once fraudsters obtain these credentials, they are more freely available than ever. Account login credentials for bank accounts

¹ Pindrop 2022 Voice Intelligence Report, available at <https://assets.pindrop.com/2022-voice-intelligence-report>

² *Id.*



with over \$2,000 in them are available for just \$65 on the dark web.³ Rather than relying on impersonal codes that may be intercepted, Pindrop's solutions return the power to the consumer in a personal, secure manner.

Our technology promises a powerful, more democratic future for the consumer, providing greater security for all while unlocking a world previously closed off to members of society such as the disabled, the elderly, and the immigrant. In short, Pindrop creates more human, impactful experiences that expand opportunities for businesses and the people they serve.

Given the omnipresent threats of identity theft and countervailing opportunities for access and security, it is both necessary and urgent to make advanced authentication and anti-fraud tools available for the benefit of consumers. Equally as necessary is ensuring that regulatory regimes do not unintentionally curtail the ability of Pindrop and other anti-fraud, pro-privacy companies from protecting California consumers and giving them the tools to protect themselves.

Pindrop recognizes and appreciates the additional focus on security and fraud purposes in these proposed regulations and believes that there are additional provisions which could further protect consumers. More specifically, we propose issuing guidance to more proportionately scope compliance obligations for B2B companies like ours – who functionally exist solely as a Service Provider under CCPA – but who, because we use a public-facing website must, for that website only, act as Business. The increasing obligations on businesses in the CPRA and these proposed regulations are diverting precious resources that should be directed to helping our customers protect California consumers and complying with California consumer requests and other CCPA obligations.

1. The Proposed Regulations Should Include More Robust Anti-Fraud Provisions that Favor Consumers and More Strongly Align with Other State Privacy Laws

Pindrop appreciates that the current draft expands the security and fraud exemption when responding to Right to Limit Sensitive Information requests, in addition to the existing exemption for Right to Delete requests. However, this still does not adequately protect California consumers because it requires providing information to individuals whom companies believe to be fraudsters that could compromise companies' defenses. For example, just alerting a fraudster that they have been detected can allow them to understand the tools being used, information being verified, or possibly even the type of company the business is using to authenticate its customers. This emboldens them to change their methods, try new authentication credentials or use additional personal information on their next try. Pindrop believes that the regulations are an opportunity to strengthen the statute in favor of consumer protection, tipping the scales to clearly favor the security and safety of the consumer. In order to achieve this posture, we advocate that all consumer rights requests should be subject to a broader security and fraud exemption that is more aligned with other state privacy statutes, enables businesses to standardize their operations to support such requests, and ensures California consumers are afforded no less protection than consumers of other states.

³ Gomez, Miguel, Dark Web Price Index 2020, Feb 2022, <https://www.privacyaffairs.com/dark-web-price-index-2020/>



This improvement is critically important.

While the current draft of the regulations permits a business to refuse a consumer rights request if they cannot identify the individual or believe the request is fraudulent, there are also numerous requirements attached to the process of refusing a request – including explaining the basis for the denial and allowing the consumer to submit additional verification, treating a Request to Correct as a Request to Delete, etc. Additionally, the existence of a third-party agent to act on the consumers’ behalf increases the risk and volume of identity theft and consumer fraud. If a business suspects that a consumer request is a fraudulent request, it should not have to provide a reason to the suspected cybercriminal. As described above, doing so would weaken businesses’ defenses against these threat actors by disclosing, even implicitly, the strength of a businesses’ defenses or the type of verification a business might use. As an example, a business providing a response to a Right to Delete request by stating it believes the request is fraudulent may encourage a hacker to obtain additional information about the consumer so as to try using different authentication factors.

A business which refuses a consumer rights request because it believes such request to be fraudulent should be able to deny the request without further explanation to the individual making the request. To help achieve more effective consumer protections, we propose the following addition to §7060:

“(i) A business that reasonably believes a consumer rights request is fraudulent, malicious, or otherwise is not made by the consumer or the consumer’s third-party agent, shall not be required to provide any additional documentation or rationale for denying the request.”

As an alternative, we propose adopting the type of anti-fraud protections that every other state privacy statute in the country permits. These allow the business to take all available measures to deter and counter fraudulent activity, and further has the benefit of being identical to each other, which promotes interoperability. It makes eminent sense for California to also strengthen cybersecurity protections for its consumers. For this alternative, the language we propose as an addition to §7060 is as follows:

“(i) Nothing in this title shall be construed to restrict a business’s, service provider’s, or contractor’s ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate report, or prosecute those responsible for any such action.”

Either or both additions would be a dramatic improvement in the ability for businesses to protect their consumers in California. Consider the costs of failing to do so: in other states with privacy statutes that do not have such an exception, such as Illinois and its Biometric Information Privacy Act (BIPA), we have seen our customers simply turn off our services, because the protections do not outweigh the costs of offering the service. Strengthening the incentive for businesses to provide fraud and identity theft protection for its citizens is a worthy and positive outcome of this regulatory process.



2. Voice Authentication Should be Considered an Element of the Required “Reasonable Security Procedures and Practices” under California Law

As this agency knows well, California requires all entities holding personal information about consumers to implement “reasonable security procedures and practices” in order to protect the data from “unauthorized access, destruction, use, modification, or disclosure.”⁴ Moreover, the CCPA permits civil lawsuits for data breaches that result from a breach of this duty.

In 2016, then-Attorney General Kamala Harris issued the foundational [California Data Breach Report](#), wherein her office outlined minimum standards for reasonable data security. The report, however, is now more than six years old, and does not reflect the most modern forms of data protection, including voice authentication. Voice authentication is far more secure – *and more consumer-friendly* – than KBA, OTP, and other commonly-used methods of authentication.⁵

This rulemaking process offers an opportunity to provide additional guidance regarding the methods of data security that qualify as “reasonable.” Section 1798.199.140(f) of the CPRA delegates to the California Privacy Protection Authority (CPPA) the responsibility to “[p]rovide guidance to businesses regarding their duties and responsibilities under this title...” Providing updated guidance to the California business community regarding minimum standards of data security that reflects the modern tools available and in use by businesses would be a very helpful exercise and help keep California in the position of leading other states (and the federal government) regarding data privacy and security practices.

3. Ease the Compliance Burden on B2B Entities that Maintain a Public-Facing Website which Consumers Are Unlikely To Visit

One of the major weaknesses in the CCPA has been that it has placed significant burdens on B2B businesses – service providers – who maintain a public-facing website. Many of these businesses, like Pindrop, use free analytics services to have a general idea of audience characteristics and numbers of those visiting such public websites. However, the CCPA’s expansive definition of “sale” means that for the purposes of the website, these service providers must act as a business, and in so doing go through the entire exercise of drafting disclosures and privacy policy modifications, operationalizing the opt-outs, drafting the various notices, etc.

This is not an efficient use of resources for entities that rarely, if ever, have consumers visit their websites. The best use of resources for these entities is ensuring that they are working with their customers – the businesses – so that they are able to assist the businesses with consumer rights requests, updating contracts for statutory compliance, and implementing and maintaining vendor compliance processes.

⁴ Cal. Civ. Code 1798.1.5(b);

⁵ <https://www.enterprisesecuritymag.com/news/multi-factor-authentication-a-leap-forward-for-call-centers-nid-1140-cid-52.html>



This draft of the regulations includes additional disclosure requirements and operational requirements for opt-outs, for which Pindrop takes no issue with for businesses that are truly consumer-facing.

For entities like Pindrop, however, we believe that a short-form disclosure and an exemption from recognizing opt-out preference signals (OPS) strikes the proper balance between acknowledging that our website may inadvertently have consumers visiting (we do not know because we do not distinguish between individuals and B2B visits) and recognizing that spending literally tens of thousands of dollars to operationalize obligations that will almost never be used due to our position in the online ecosystem is not a good use of time or money.

This short-form disclosure should contain a concise summary of the information that is collected, along with a list of the rights that consumers have under the CCPA. Additionally, the disclosure could require the entity to state whether it recognizes an OPS or not. This type of common-sense limitation to the CCPA/CPRA requirements would be welcomed by the business community as a recognition of the financial and time burdens spent on efforts that are very unlikely to benefit consumers.

Of course, to prevent this from being construed or used as a loophole for entities that truly serve as both businesses and service providers, Pindrop would propose that this option be limited to Service Providers who must act as a Business only to the extent they have a website or mobile application, and who have fewer than 10,000 combined unique visitors or downloads from California to their online presence in a calendar year. Only eligible companies would then be permitted to design and use short-form disclosures describing CCPA rights and information collected, and be exempt from recognizing OPS.

Pindrop thanks you for the opportunity to comment on these draft regulations. We are keenly interested in the safety of California consumers, and these proposed modifications aim to increase the protections included in the CCPA (as amended by the CPRA). We would be delighted to discuss any of these proposed changes further.



Clarissa Cerda
Chief Legal Officer
Pindrop Security, Inc.

From: **Dan Frechtling** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 22.08.2022 16:45:11 (+02:00)
Attachments: Dan Frechtling Boltive CPPA public comment Aug 23^J 2022.pdf (7 pages), Dan Frechtling Boltive CPPA public comment Aug 23, 2022.docx (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

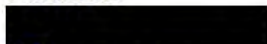
Thank you for the invitation for preliminary comments on CPRA proposed rulemaking. Please find attached my comments as the CEO of a privacy technology company doing business in California. I am providing the same document in both Word and PDF format for your convenience.

Please advise of any questions I may answer.

Best,
Dan

--

Dan Frechtling
CEO
Boltive



--

Dan Frechtling, CEO



August 22, 2022
 California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd.,
 Sacramento, CA 95834

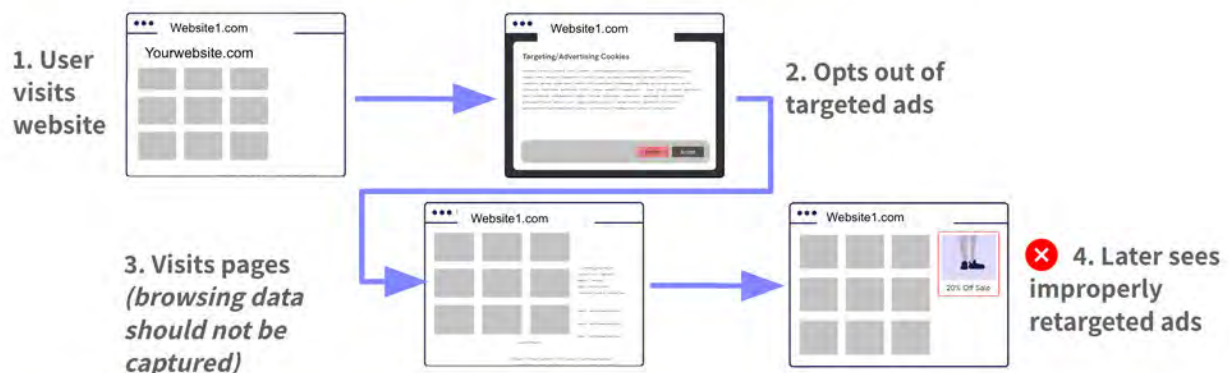
Re: CPPA PUBLIC COMMENT REGARDING PROPOSED REGULATIONS FOR THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Mr. Soublet,

Boltive, a privacy technology company doing business in California, appreciates the opportunity to comment on Proposed Regulations Under the California Privacy Rights Act. We thank the California Privacy Protection Agency for seeking input from stakeholders in developing regulations.

Over five years, Boltive software has been used by hundreds of online companies to identify and block malicious and non-compliant advertising. We monitor 100 billion ad impressions per month. Recently, many of our clients have asked us to help them comply with data privacy regulations because they understand the risks posed by consent errors (see Figure 1).

The Average US Consumer Faces Up To 100 Consent Errors Per Day



Unwanted retargeted ads are visible. The root-cause—consent errors—is invisible. The average US consumer has 750 bid requests daily, and a 1/3 CMP error rate.

Source: Boltive Software, Irish Council for Civil Liberties

Figure 1

Our software utilizes synthetic personas as secret shoppers for data privacy compliance. We enable companies to audit and remediate their practices so they follow CCPA/CPRA terms. Somewhat surprisingly, over 90% of the companies we work with find consent flaws that could cause unauthorized data selling or sharing. We believe our findings can be useful to the current rulemaking process.

We are pleased with the changes the CPPA has made in the rules, especially regarding third parties in 7026, 7051 and 7053. However, we believe the Agency can improve 7026 and 7053 to provide better consumer protection.

Our comments can be summarized in four areas:

- 1. We strongly support the recognition in 7053(b) and 7026(f) that third parties and similar intermediaries bear responsibility for honoring and transmitting opt-out signals.**
- 2. We believe that certain clauses in 7051 that apply to service providers should also be included in 7053 to apply to third parties.**
 - a. Reviews, audits and scans of service providers in 7051(a)(7) also should refer to third parties in 7053(a)(4).**
 - b. Safe harbor clarifications applying to service providers in 7051(e) also should apply to third parties in 7053(e).**
- 3. We disagree with the declaration in 7026(a)(4) that cookie banners and controls are not acceptable methods for opt-outs.**
- 4. We believe businesses, service providers and third parties should be required to make it easy for consumers to withdraw consent.**

1. We strongly support the recognition in 7053(b) and 7026(f) that third parties and similar intermediaries bear responsibility for honoring and transmitting opt-out signals.

Section 7053(b) helps ensure businesses contract with third parties to check and honor consumer opt-outs. In some cases, businesses have authorized third parties to act behalf of businesses or for their own purposes.

Section 7026(f) states the obligations to businesses and third parties to pass opt-outs throughout the chain of vendors. In 7026(f)(2)-(3), when a consumer requests to opt-out, businesses must notify all third parties and “forward the request to any other person” with whom personal information has been disclosed or shared. Section 7026(f)(4) calls for a confirmation signal, defined as “providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business.”

These are critical points because of the prevalence of what we call “dark signals.” Consumer opt-outs are mis-transmitted between the chain of cross-context behavioral advertising vendors over one-third of the time. This means opt-out signals elected by consumers are lost in the series of technical hand-offs between adtech vendors, causing consumer harm as data is shared illegitimately. We illustrated dark signals in a prior written submission November 5, 2021, and spoken testimony to the CPPA on May 5, 2022

The problem of failed opt-outs largely rests with lesser-known third parties in cross-context behavioral advertising. These are more often intermediaries in the consent chain rather than the better-known advertisers and publishers.

Privacy and security go together. CPRA rules follow security principles from CCPA and the California OAG requiring companies to implement reasonable security procedures. These principles include “reasonable security measures” that are different for online advertising than email and are described in CCPA FSOR Appendix A at 134 (response 431) and at 311 (responses 431, 924).

We strongly support the regulations as currently drafted and encourage the CPPA to leave them unamended.

2. We believe that certain clauses in 7051 that apply to service providers should also be included in 7053 to apply to third parties

Statements referring to reviews, audits and scans of service providers in 7051(a)(7) should also refer to third parties in 7053(a)(4). We welcome 7051, where various contract provisions are consolidated. Further, under 7051(a)(7), contracts between businesses and service providers or contractors grant a business the right to undertake “ongoing manual reviews and automated scans of the service provider’s system and regular assessments, audits, or other technical and operational testing at least once every 12 months.”

We are puzzled as to why this language is missing from 7053(a)(4), which merely states a “business may require the third party to attest” to their compliance. It is not clear to us why third parties are granted relief from the reasonable and appropriate steps in 7051(a)(7).

In our software trials with dozens of online brands, we’ve found the greatest vulnerabilities in data sharing come from transmissions to third parties for cross-context behavioral advertising. These vulnerabilities have been overcome through the evidence from our software audits. The best way to ensure third parties don’t misuse personal data is to require businesses to audit them.

The safe harbor clarifications applying to service providers in 7051(e) also should apply to third parties in 7053(e). You have wisely updated rules in 7051(e) and 7053(e) and are closing loophole in CCPAs. Ignorance of lapses by service providers, contractors, or third parties should not be a defense. But section 7053(e) addressing third parties should carry the same language as section 7051(e) addressing service providers.

Section 7051(e) makes it clear there is no safe harbor with service providers if you don't exercise audit rights. It states, "a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA"

In 7053(e), which applies to third parties, the statement is similar, but omits "exercises its rights to audit or test the [third party's] systems." Instead, the business is advised simply to enforce its contract with the third party. We propose you add the audit and test language to ensure best practice.

In our analysis of opt-out consent failure rates, handoffs from the business to third parties or in between third parties is a greater source of errors than the hand-off from consent management platforms. In fact, third-party consent handoffs fail 24% of the time (see Figure 2). These handoffs continue to be grey areas of deniability. The solution is to apply the language from 7051(a)(7) and 7051(e) to the appropriate clauses that apply to third parties in section 7053.

Online Publishers Using CMPs Experience 37% Error Rate Across Vendors



Consent vendors and network partners both may mis-transmit personal data...causing dark signals...if they are not audited

Source: Boltive software and analysis

Figure 2

One might argue against our two recommendations on the grounds that testing and auditing third parties creates an unfair burden to businesses. Fortunately, the necessary scanning can be accomplished with low-cost software automation that avoids a manual burden on companies.

3. We disagree with the 7026(a)(4) declaration that cookie banners and controls are not acceptable methods for opt-outs.

The ISOR explanation for the rejection is because they “concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.”

We disagree with this interpretation because preference centers commonly bundled with cookie banners can integrate with on-page tags and cross-context behavioral advertising vendors to address the sale and sharing of personal information.

Furthermore, cookie banners are a widely accepted method of opting out, particularly with cross-context behavioral advertising. Our data shows these technologies have limitations, but they are correctable. We are unaware of other commonly used methods for opting out of OBA that are superior. If web publishers opt for homegrown solutions, consent is even more likely to be lost than if solutions by specialist vendor are used.

We understand this method may be insufficient with respect to other forms of data sharing such as through data brokers. But we urge the CPPA to reconsider the interpretation cookie banners and controls are not acceptable for advertising opt outs.

4. We believe businesses, service providers and third parties should be required to make it easy for consumers to withdraw consent, which may be added to 7002.

Consumers may change their minds about data sharing for any number of reasons. Their life circumstances may change. Businesses may add intrusive terms to their privacy policies. Fortunately, other laws have provided language we can reference.

GDPR has consent revocation as a definitive right. Article 7 of the GDPR expressly states that a “data subject shall have the right to withdraw his or her consent at any time.”

The CTDPA, Connecticut’s consumer privacy law, specifically states users have the right to revoke consent. Exercising this right must be easy, “at least as easy as the mechanism by which the consumer provided the consumer’s consent” (Section 6(6)). Upon revocation, the

controller as defined under Connecticut law must stop processing data as soon as feasible, but no later than 15 days after receipt of request.

Finally, as of this writing the draft text of the American Data Privacy and Protection Act (ADPPA) says a company must “provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided” (Section 204(a)).

We do not see this clause in the CCPA revised language. We recommend adding it to 7002(a). Requiring businesses to honor withdrawal of consent at any time recognizes consent, like nearly every agreement between individuals and businesses, is not permanent and irreversible.

Closing

Failing to hold third parties accountable creates far more issues than just consumer inconvenience. Unauthorized data sharing can reach malware providers and even sanctioned entities (see Figure 3).

Unaudited Third Parties Can Leak Consumer Data To Malicious Parties

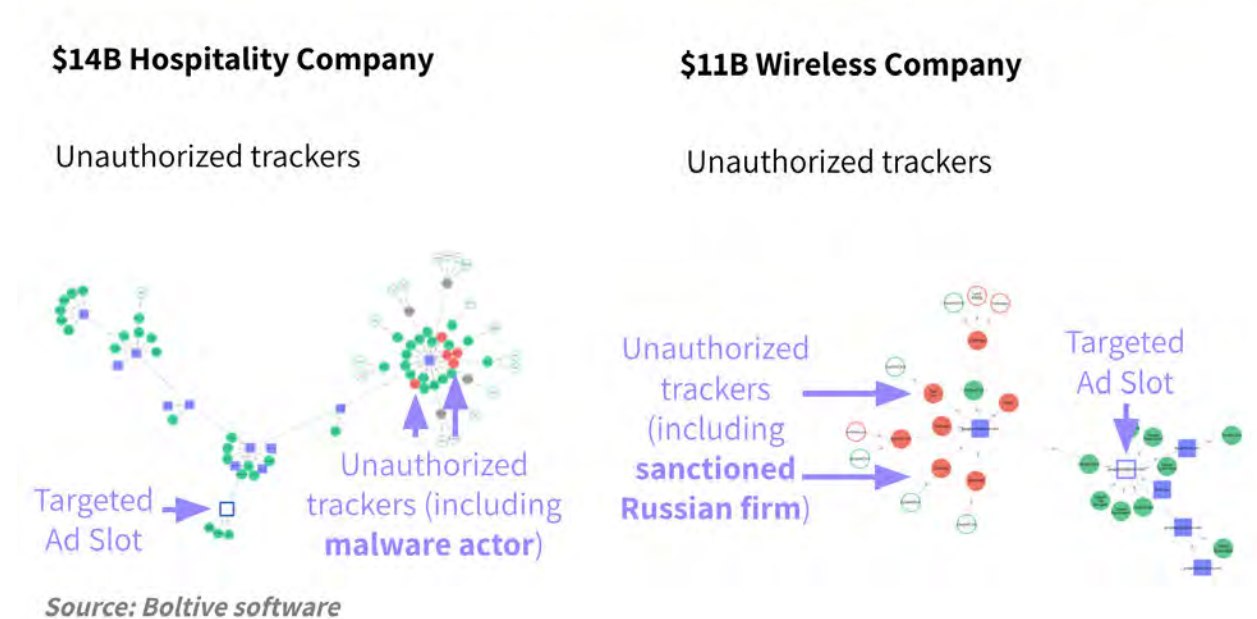


Figure 3

We continue to monitor and gather data around consent opt-outs and unauthorized data collectors so companies can comply with CCPA, CPRA, and industry standards such as generally accepted privacy principles (GAPP), privacy by design, and the

like. Thank you for consideration of our comments. Please do not hesitate to reach out if you have any questions.

Respectfully submitted,



Dan Frechtling
CEO, Boltive

August 22, 2022
 California Privacy Protection Agency
 Attn: Brian Soubllet
 2101 Arena Blvd.,
 Sacramento, CA 95834

Re: CPPA PUBLIC COMMENT REGARDING PROPOSED REGULATIONS FOR THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Mr. Soubllet,

Boltive, a privacy technology company doing business in California, appreciates the opportunity to comment on Proposed Regulations Under the California Privacy Rights Act. We thank the California Privacy Protection Agency for seeking input from stakeholders in developing regulations.

Over five years, Boltive software has been used by hundreds of online companies to identify and block malicious and non-compliant advertising. We monitor 100 billion ad impressions per month. Recently, many of our clients have asked us to help them comply with data privacy regulations because they understand the risks posed by consent errors (see Figure 1).

The Average US Consumer Faces Up To 100 Consent Errors Per Day



Unwanted retargeted ads are visible. The root-cause—consent errors—is invisible. The average US consumer has 750 bid requests daily, and a 1/3 CMP error rate.

Source: Boltive Software, Irish Council for Civil Liberties

Figure 1

Our software utilizes synthetic personas as secret shoppers for data privacy compliance. We enable companies to audit and remediate their practices so they follow CCPA/CPRA terms. Somewhat surprisingly, over 90% of the companies we work with find consent flaws that could cause unauthorized data selling or sharing. We believe our findings can be useful to the current rulemaking process.

We are pleased with the changes the CPPA has made in the rules, especially regarding third parties in 7026, 7051 and 7053. However, we believe the Agency can improve 7026 and 7053 to provide better consumer protection.

Our comments can be summarized in four areas:

- 1. We strongly support the recognition in 7053(b) and 7026(f) that third parties and similar intermediaries bear responsibility for honoring and transmitting opt-out signals.**
- 2. We believe that certain clauses in 7051 that apply to service providers should also be included in 7053 to apply to third parties.**
 - a. Reviews, audits and scans of service providers in 7051(a)(7) also should refer to third parties in 7053(a)(4).**
 - b. Safe harbor clarifications applying to service providers in 7051(e) also should apply to third parties in 7053(e).**
- 3. We disagree with the declaration in 7026(a)(4) that cookie banners and controls are not acceptable methods for opt-outs.**
- 4. We believe businesses, service providers and third parties should be required to make it easy for consumers to withdraw consent.**

1. We strongly support the recognition in 7053(b) and 7026(f) that third parties and similar intermediaries bear responsibility for honoring and transmitting opt-out signals.

Section 7053(b) helps ensure businesses contract with third parties to check and honor consumer opt-outs. In some cases, businesses have authorized third parties to act behalf of businesses or for their own purposes.

Section 7026(f) states the obligations to businesses and third parties to pass opt-outs throughout the chain of vendors. In 7026(f)(2)-(3), when a consumer requests to opt-out, businesses must notify all third parties and “forward the request to any other person” with whom personal information has been disclosed or shared. Section 7026(f)(4) calls for a confirmation signal, defined as “providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business.”

These are critical points because of the prevalence of what we call “dark signals.” Consumer opt-outs are mis-transmitted between the chain of cross-context behavioral advertising vendors over one-third of the time. This means opt-out signals elected by consumers are lost in the series of technical hand-offs between adtech vendors, causing consumer harm as data is shared illegitimately. We illustrated dark signals in a prior written submission November 5, 2021, and spoken testimony to the CPPA on May 5, 2022

The problem of failed opt-outs largely rests with lesser-known third parties in cross-context behavioral advertising. These are more often intermediaries in the consent chain rather than the better-known advertisers and publishers.

Privacy and security go together. CPRA rules follow security principles from CCPA and the California OAG requiring companies to implement reasonable security procedures. These principles include “reasonable security measures” that are different for online advertising than email and are described in CCPA FSOR Appendix A at 134 (response 431) and at 311 (responses 431, 924).

We strongly support the regulations as currently drafted and encourage the CPPA to leave them unamended.

2. We believe that certain clauses in 7051 that apply to service providers should also be included in 7053 to apply to third parties

Statements referring to reviews, audits and scans of service providers in 7051(a)(7) should also refer to third parties in 7053(a)(4). We welcome 7051, where various contract provisions are consolidated. Further, under 7051(a)(7), contracts between businesses and service providers or contractors grant a business the right to undertake “ongoing manual reviews and automated scans of the service provider’s system and regular assessments, audits, or other technical and operational testing at least once every 12 months.”

We are puzzled as to why this language is missing from 7053(a)(4), which merely states a “business may require the third party to attest” to their compliance. It is not clear to us why third parties are granted relief from the reasonable and appropriate steps in 7051(a)(7).

In our software trials with dozens of online brands, we’ve found the greatest vulnerabilities in data sharing come from transmissions to third parties for cross-context behavioral advertising. These vulnerabilities have been overcome through the evidence from our software audits. The best way to ensure third parties don’t misuse personal data is to require businesses to audit them.

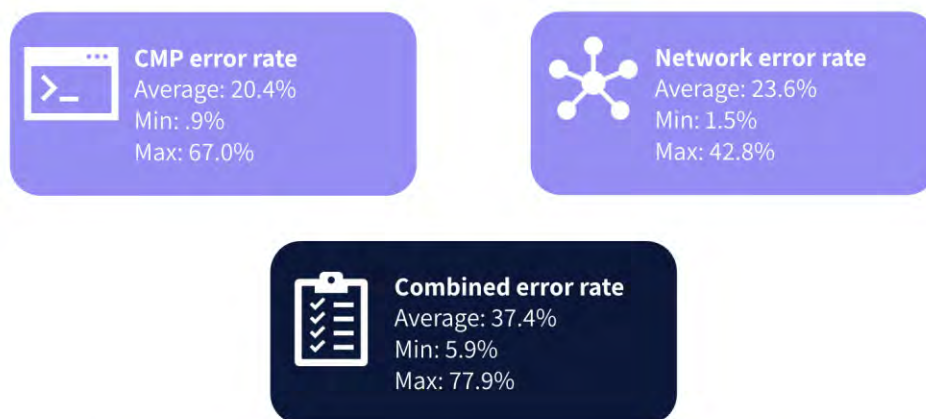
The safe harbor clarifications applying to service providers in 7051(e) also should apply to third parties in 7053(e). You have wisely updated rules in 7051(e) and 7053(e) and are closing loophole in CCPAs. Ignorance of lapses by service providers, contractors, or third parties should not be a defense. But section 7053(e) addressing third parties should carry the same language as section 7051(e) addressing service providers.

Section 7051(e) makes it clear there is no safe harbor with service providers if you don't exercise audit rights. It states, "a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA"

In 7053(e), which applies to third parties, the statement is similar, but omits "exercises its rights to audit or test the [third party's] systems." Instead, the business is advised simply to enforce its contract with the third party. We propose you add the audit and test language to ensure best practice.

In our analysis of opt-out consent failure rates, handoffs from the business to third parties or in between third parties is a greater source of errors than the hand-off from consent management platforms. In fact, third-party consent handoffs fail 24% of the time (see Figure 2). These handoffs continue to be grey areas of deniability. The solution is to apply the language from 7051(a)(7) and 7051(e) to the appropriate clauses that apply to third parties in section 7053.

Online Publishers Using CMPs Experience 37% Error Rate Across Vendors



Consent vendors and network partners both may mis-transmit personal data...causing dark signals...if they are not audited

Source: Boltive software and analysis

Figure 2

One might argue against our two recommendations on the grounds that testing and auditing third parties creates an unfair burden to businesses. Fortunately, the necessary scanning can be accomplished with low-cost software automation that avoids a manual burden on companies.

3. We disagree with the 7026(a)(4) declaration that cookie banners and controls are not acceptable methods for opt-outs.

The ISOR explanation for the rejection is because they “concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.”

We disagree with this interpretation because preference centers commonly bundled with cookie banners can integrate with on-page tags and cross-context behavioral advertising vendors to address the sale and sharing of personal information.

Furthermore, cookie banners are a widely accepted method of opting out, particularly with cross-context behavioral advertising. Our data shows these technologies have limitations, but they are correctable. We are unaware of other commonly used methods for opting out of OBA that are superior. If web publishers opt for homegrown solutions, consent is even more likely to be lost than if solutions by specialist vendor are used.

We understand this method may be insufficient with respect to other forms of data sharing such as through data brokers. But we urge the CPPA to reconsider the interpretation cookie banners and controls are not acceptable for advertising opt outs.

4. We believe businesses, service providers and third parties should be required to make it easy for consumers to withdraw consent, which may be added to 7002.

Consumers may change their minds about data sharing for any number of reasons. Their life circumstances may change. Businesses may add intrusive terms to their privacy policies. Fortunately, other laws have provided language we can reference.

GDPR has consent revocation as a definitive right. Article 7 of the GDPR expressly states that a “data subject shall have the right to withdraw his or her consent at any time.”

The CTDPA, Connecticut’s consumer privacy law, specifically states users have the right to revoke consent. Exercising this right must be easy, “at least as easy as the mechanism by which the consumer provided the consumer’s consent” (Section 6(6)). Upon revocation, the

controller as defined under Connecticut law must stop processing data as soon as feasible, but no later than 15 days after receipt of request.

Finally, as of this writing the draft text of the American Data Privacy and Protection Act (ADPPA) says a company must “provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided” (Section AA 204(a)).

We do not see this clause in the CCPA revised language. We recommend adding it to 7002(a). Requiring businesses to honor withdrawal of consent at any time recognizes consent, like nearly every agreement between individuals and businesses, is not permanent and irreversible.

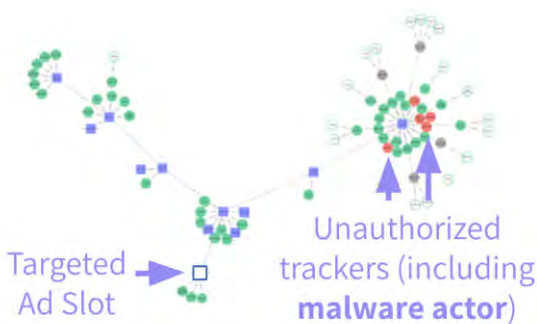
Closing

Failing to hold third parties accountable creates far more issues than just consumer inconvenience. Unauthorized data sharing can reach malware providers and even sanctioned entities (see Figure 3).

Unaudited Third Parties Can Leak Consumer Data To Malicious Parties

\$14B Hospitality Company

Unauthorized trackers



Source: Boltive software

\$11B Wireless Company

Unauthorized trackers

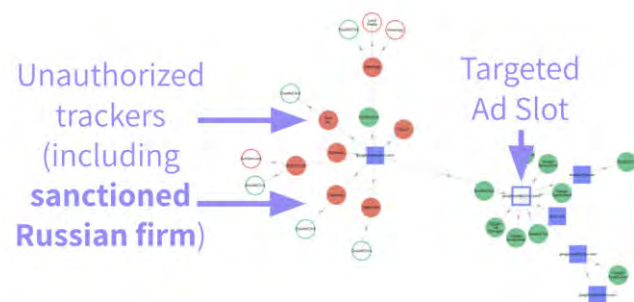


Figure 3

We continue to monitor and gather data around consent opt-outs and unauthorized data collectors so companies can comply with CCPA, CPRA, and industry standards such as generally accepted privacy principles (GAPP), privacy by design, and the

like. Thank you for consideration of our comments. Please do not hesitate to reach out if you have any questions.

Respectfully submitted,



Dan Frechtling
CEO, Boltive

From: Shelton Leipzig, Dominique [REDACTED]
To: Regulations <Regulations@coppa.ca.gov>
Keck, Sasha L. [REDACTED] Kourinian, Arsen
; Leyva, Britteny L.
CC: [REDACTED]; Von Borstel, Megan
[REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 00:04:03 (+02:00)
Attachments: CalChamber CPRA Regulations Letter_08-22-2022.pdf (49 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Greetings,

On behalf of the California Chamber of Commerce (CalChamber), please find attached CalChamber's comments regarding the proposed California Privacy Rights Act regulations.

With very best regards,
Dominique

Dominique Shelton Leipzig

Partner, Cybersecurity & Data Privacy

Leader, Global Data Innovation and Ad Tech Privacy & Data Management practices

Pronouns: she/her

Mayer Brown

350 S. Grand Ave #2500

Los Angeles, California 90071

[REDACTED]
[LinkedIn](#) [Twitter](#)

mayerbrown.com

August 22, 2022

Mayer Brown LLP
 350 South Grand Avenue
 25th Floor
 Los Angeles, CA 90071-1503
 United States of America

T: +1 213 229 9500
 F: +1 213 625 0248

mayerbrown.com

Dominique Shelton Leipzig
 Partner

California Chamber of Commerce Comments to Draft California Privacy Rights Act Regulations

INTRODUCTION

The California Chamber of Commerce (CalChamber) respectfully submits these comments to the California Privacy Protection Agency's (the Agency) July 8, 2022, [Notice of Proposed Rulemaking](#) regarding the [proposed California Privacy Rights Act \(CPRA\) regulations](#). In sum, CalChamber requests the following modifications to the proposed CPRA regulations, which are described in greater detail below in the Comments section:

1. **The Agency Should Postpone Enforcement of the CPRA Because of the Agency's Delay in Finalizing the CPRA Regulations.** Under the CPRA, the dates set for finalizing the regulations (July 1, 2022) and start of enforcement (July 1, 2023) provided a one-year compliance window. The one-year window reflected the time needed for businesses to assess and implement changes necessary to comply with new requirements. Because the Agency has not met the deadline to finalize the regulations, enforcement should be postponed to one year after the CPRA regulations are finalized.
2. **The "Average Consumer" Standard Proposed in Section 7002 Is Contrary to the CPRA and Deviates from the Approach Established in Other Privacy Laws.** We propose revisions to remove the "average consumer" standard and align restrictions on the collection and use of personal information to the language in the CPRA. The CPRA standard evaluates the collection of personal information based on the reasonableness of a business's processing activities and transparency, not the ambiguous expectations of an "average consumer." Moreover, the proposed regulation could shift California from an implied consent based on notice jurisdiction to an opt-in jurisdiction, which is contrary to California law. In addition to deviating from California law, adopting the "average consumer" standard would separate California from the EU's General Data Protection Regulation (GDPR) and other state privacy laws that apply the reasonableness approach set out in the text of the CPRA.
3. **Methods for Honoring Opt-Out Preferences Should Remain Flexible and Facilitate Consumer Choice as Intended by the CPRA.** As proposed, section 7025's mandate that businesses honor opt-out preference signals *and* provide an opt-out link contravenes the

August 22, 2022

Page 2

CPRA statute, which gives businesses flexibility to choose either option without requiring both. The proposed regulation further contradicts the CPRA by adding that a business is only able to employ opt-out preference signals, without providing the opt-out link, if they do so in a “frictionless manner,” a term not used in the CPRA. We propose modifications to rectify this misalignment with the CPRA and to incorporate CPRA requirements intended to facilitate consumer choice, such as the requirement to be free of defaults that presuppose consumer intent, and avoiding conflicts with commonly used privacy settings. These changes encourage consumer choice without removing the flexibility for businesses that the CPRA intended.

- 4. The Proposed Requirements for Handling Opt-Outs of Sale and Sharing Should Be Revised To Limit Burdens on Business that Do Not Materially Benefit Consumers.** We propose two changes to section 7026 to address unnecessary requirements. First, we request changes to make clear that section 7026 requires businesses to honor opt-out requests on a going-forward basis. As written, the proposed regulation could create ambiguity around applicability of this requirement. In an abundance of caution, businesses may seek to implement requests retroactively, which would involve a “disproportionate effort,” as set forth in section 7001(h), and impose a significant burden on businesses to try to unwind prior data transactions, even though consumers did not previously object to those transactions. Second, businesses should not be required to display consumer preferences on the webpage, as this would unnecessarily clutter the user experience, be technologically difficult to implement, and may lead to confusion. Consumers are sufficiently served by showing the preferences within the privacy settings.
- 5. Requirements To Prevent Dark Patterns Should Be Tailored To Address Fraudulent Practices Without Undermining Consumer Choice.** As proposed, section 7004 risks undermining consumer choice with ambiguous and overly restrictive standards, as well as potentially running afoul of First Amendment protections that allow businesses to share truthful and accurate information with consumers. We request that the Agency add reasonable limits and focus on requirements that give businesses flexibility to adopt practical and appropriate methods for informing consumers about their choices, while prohibiting potentially fraudulent practices.
- 6. Notice of Collection Requirements Should Be Reasonable To Avoid Becoming Cumbersome and Duplicative.** Draft section 7012 sets out additional requirements for notices of collection when more than one party is involved. We propose modifications to these requirements in line with the CPRA and GDPR to limit cumbersome and duplicative disclosures. First, we urge the Agency to remove the requirement that a business’s privacy notice list all third-party names. The CPRA only requires that a business disclose the categories of third parties, which serves the purpose of informing consumers without making the notice unwieldy and imposing unnecessary burdens on businesses. Second, the proposed requirement that all parties involved provide notice should be revised to align

August 22, 2022

Page 3

with the GDPR. Under the GDPR, joint controllers allocate responsibilities for compliance amongst themselves, including the obligation to provide a privacy notice. Duplicative disclosures are confusing and run the risk of being tuned out by consumers.

- 7. The Agency’s Authority To Conduct Audits Should Be Subject To Reasonable Limits.** As drafted, the Agency has broad power to audit a business without evidence of a violation and without any notice to the business. Responding to audits can take resources away from valuable compliance efforts and yield little benefit to consumers when the Agency does not have concrete indications of wrongdoing by the business. Moreover, when the business does not have any notice of an audit, the Agency may obtain an incorrect impression of the business’s compliance if the business has not had sufficient time to assemble responses to the Agency’s requests. The Agency’s audits should be limited to instances where it has sufficient facts to support the audit and are clearly defined in advance; the Agency should also provide the business with 60 days’ notice to ensure that the audit can be efficiently managed.
- 8. While Organizing Requirements for Service Provider and Contractor Agreements Is Valuable, Any Additional Requirements the Agency Is Seeking To Add Should Be Crafted To Benefit Consumers Without Unduly Burdening Businesses.** As drafted, the regulations create potential confusion and impose overly restrictive contractual requirements unnecessary to achieve the purpose of the CPRA. For example, the draft regulations should be modified to clarify that the CPRA does not apply to entities that process personal information on behalf of non-businesses (e.g., nonprofits and government entities). We also propose modifications to sections 7050, 7051, and 7053 to align the obligations of service providers and contractors with the CPRA statute and to address unnecessarily prescriptive and onerous requirements.
- 9. Notice Requirements in Connection with Phone Calls and Smart Devices Should Be Designed To Better Serve Both Consumer Privacy and the User Experience.** Draft section 7013 requires businesses to ensure that consumers encounter a privacy notice while contacting a business over the phone or using a smart device. The notice requirements in connection with phone calls and smart devices should focus on whether consumers can *access* the privacy notice, not whether they will *encounter* the notice on call or smart devices. This will better serve consumer privacy, creating a meaningful opportunity to review the notice, without disrupting the consumer experience.
- 10. The Agency Should Accommodate the Possibility of Opt-In Consent for the Use of Sensitive Personal Information and Remove Excessively Restrictive Requirements That Do Not Materially Benefit Consumers.** We propose two modifications to sections 7014 and 7015 regarding the requirements for sensitive personal information. Rather than providing a notice of the right to limit processing, businesses that want to take a more privacy-protective approach should have the option to obtain opt-in consent before processing sensitive personal information for a purpose other than the purposes enumerated

August 22, 2022

Page 4

in the statute. This proposal is more privacy protective in honoring consumer choice. Second, the draft requirement that the icon size on the business's website be the same size as others on the page is unduly burdensome to implement in practice. A flexible approach achieves the goals of providing consumers with information without creating an unwieldy standard.

- 11. Requirements Related to Responding to Requests To Delete Should Be Reasonable To Achieve the Purposes of the CPRA Without Imposing Resource-Intensive Processes.** We request that the Agency consider removing requirements that (1) businesses, service providers, and contractors provide a detailed explanation regarding why notification would be impossible or involve disproportionate effort and (2) businesses explain to consumers the exemption they are relying on in denying a deletion request. Providing these explanations is time- and resource-intensive. Businesses would struggle to allocate sufficient resources and labor to handle such explanations if required. Moreover, the CPRA does not mandate that businesses provide detailed explanations. Imposing this additional requirement on businesses is not necessary to implement the CPRA.
- 12. The Proposed Requirement that Businesses Notify Service Providers and Contractors of a Consumer's Request To Correct Exceeds the Agency's Authority Under the CPRA.** The CPRA does not require that businesses notify service providers and contractors of a consumer's request to correct. We request that the Agency strike this requirement or, in the alternative, add an exception to the draft regulation for when providing notice is impossible or requires disproportionate effort.
- 13. The Regulations Should Properly Place the Burden on the Consumer To Make a Specific Request for Information Exceeding the Prior 12 Months, Consistent with the CPRA.** The CPRA does not require a business to automatically provide a consumer personal information beyond the 12-month look-back period. As written, section 7024(h) could create confusion around the time period for which a business must provide data. We propose changes to clarify and align section 7024(h) of the regulations with the CPRA statute, allowing businesses the flexibility to either automatically provide personal information beyond the 12-month look-back period or choose to notify consumers that they can request personal information beyond the 12-month period and comply upon such request.
- 14. The Regulations on Requests To Limit the Use or Disclosure of Sensitive Information Should Be Revised To Align with the Text of the CPRA Statute, Avoid Undermining Consumer Choice, and Support Efforts To Combat Crime.** We have proposed a series of modifications to section 7027. First, as drafted, section 7027 sets out requirements that are not aligned with the text of the CPRA statute. We also are concerned with presenting options to consumers that result in a single option being presented more prominently than more nuanced options. This subverts consumer choice and impedes sharing truthful and accurate information. The exception for use to combat malicious, deceptive, fraudulent, or

August 22, 2022

Page 5

illegal actions should not be limited to only actions “directed at the business,” as proposed. This limits the ability of businesses to aid others that are targets of such actions by disclosing sensitive information needed to stop such actions.

- 15. Procedures for Probable Cause Proceedings Should Be Modified To Give Businesses an Opportunity To Respond To Allegations Before Initiating a Proceeding.** Before initiating a probable cause proceeding, businesses should have an opportunity to receive the information underlying the alleged violations and to provide a response, as well as to appeal or request a correction in a decision. This gives the Agency and businesses an opportunity to exchange critical information to fully inform a decision and address any errors in the decision.

COMMENTS

- 1. The Agency Should Postpone Enforcement of the CPRA Because of the Agency’s Delay in Finalizing the CPRA Regulations.**

We request that the Agency delay enforcement of the CPRA and the regulations. Under the CPRA, regulations were set to be finalized by July 1, 2022. *See* Cal. Civ. Code § 1798.185(d). The voters intended to provide a one-year compliance window ahead of the July 1, 2023, CPRA enforcement date. *Id.* Postponing enforcement is appropriate here because the Agency has not fulfilled its obligation to finalize the CPRA regulations by the July 1, 2022, deadline, and businesses need sufficient time to revise policies and procedures and implement changes to digital properties.

Indeed, contrary to the Economic Impact Statement released as part of this rulemaking, implementing compliance with the CPRA will not cost \$127.50 per business and increase labor requirements by 1.5 hours per business. *See* [Economic and Fiscal Impact Statement](#). Rather, based on a survey of the businesses that are members of CalChamber, all respondents estimated that the costs of implementing CPRA compliance will far exceed the Agency’s estimates, to the tune of hundreds of thousands of dollars, if not \$5 million or more using *conservative* estimates for larger companies. The respondents indicated that compliance efforts will necessarily involve no fewer than 300 hours, with most respondents providing estimates in the four-digit range and requiring anywhere from one to five new full-time employees per business. At a minimum, compliance legal fees *alone* would far surpass the Agency’s estimates. Compliance will require businesses to dedicate considerable time for data identification and mapping, review and revision of data policies and security measures for non-employee data, and implementation of internal training programs, among other programming, record-keeping, and reporting measures.

Businesses are also left in a precarious situation, as they are interested in implementing their CPRA compliance programs as soon as possible but cannot do so because the regulations, which contain critical details and new requirements of the CPRA, are not yet final. Accordingly, we ask the Agency to postpone the enforcement date to one year after the CPRA regulations become finalized.

August 22, 2022

Page 6

2. The “Average Consumer” Standard Proposed in Section 7002 Is Contrary to the CPRA and Deviates from the Approach Established in Other Privacy Laws (Section 7002).

A. Proposed Modifications

We propose the below modifications to section 7002(a). We also propose removing the illustrative examples in section 7002(b) or modifying section 7002(b) to align with these proposed changes to section 7002(a).

- (a) A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be used for other ~~disclosed~~ purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ any purpose that is disclosed at the time of collection. A business shall notify the consumer ~~obtain the consumer’s explicit consent~~ in accordance with section ~~70127004~~ before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that is unrelated to or incompatible with the disclosed purpose(s) for which the personal information is collected or processed.

B. Reasons for Proposed Modifications

We offer modifications to section 7002(a)–(b) to align with the CPRA and other state privacy laws.

As an initial matter, the “average consumer” standard in section 7002 should be removed. This proposed standard conflicts with the CPRA, which requires the collection of personal information to be “reasonably necessary and proportionate to achieve the purposes for which personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected” Cal. Civ. Code § 1798.100(c); *see also* 11 CCR § 7003 (providing detailed requirements for disclosures to consumers). The CPRA standard is based on the reasonableness of the business’s processing activities based on transparency, rather than an “average consumer” standard. As a result, the introduction of an “average consumer” standard may create ambiguity for CPRA compliance. A business, consumer, and regulator may have differing views on what an “average consumer” expects, particularly in California, which does not have a homogenous consumer base and has a wide variety of industries. This lack of clarity creates challenges for businesses working to comply with the regulation. It also gives the Agency broad leeway to substitute its own judgment of what is necessary and proportionate. Instead of looking to an “average consumer,” we propose language that aligns with

August 22, 2022

Page 7

the CPRA and other privacy laws and reduces ambiguity for businesses when assessing their compliance.

Further, this proposed regulation could shift California from an implied consent based on notice to an opt-in jurisdiction, which is contrary to California law. *See* Cal. Civ. Code § 1798.100(a). The CPRA, like other state privacy laws, established that California does not require consumers (except for sale of children’s data) to opt-in to data collection and use practices. *See id.* Rather, the CPRA looks to the notice provided to the consumer, and use that is compatible with that notice, to assess whether the collection is permissible. *See id.* (A business shall inform consumers of “[t]he categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes **that are incompatible with the disclosed purpose** for which the personal information was collected without providing the consumer with notice consistent with this section.”) (emphasis added). As written, draft section 7002 changes the statute by requiring consent based on the expectation of the “average consumer,” instead of the context of the collection, including the notice at or before the point of collection to consumers, along with compatible purposes. To avoid this conflict with the CPRA, we recommend that the Agency amend the draft regulation as proposed. Simply put, the disclosed purpose for collecting the consumer’s personal information is an important element in setting consumer expectations; there is no need to add an “average consumer” standard that seemingly would allow the Agency to disregard the disclosures that businesses provide to consumers.

Indeed, the GDPR does not take this approach. *See* GDPR, Arts. 5(1)(b), 13 & 14. Other state privacy laws taking effect in 2023 also do not adopt an “average consumer” approach for the purpose limitation doctrine. *See* Va. Code Ann. § 59.1-574(A)(1) (“A controller shall: Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, **as disclosed** to the consumer. . . .”) (emphasis added); Colo. Rev. Stat § 6-1-1308(c)(3) (“A controller’s collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to **the specified purposes** for which the data are processed.”) (emphasis added); Conn. Gen. Stat. § 6(a) (“A controller shall (1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, **as disclosed** to the consumer.”) (emphasis added). Adopting an “average consumer” standard would conflict with these other privacy laws, contrary to the Agency’s statement that the proposed regulations are intended to be harmonious with other privacy laws. *See* [Notice of Proposed Rulemaking](#) at 7 (“Finally, the proposed regulations take into consideration privacy laws in other jurisdictions and implement compliance with the CCPA in such a way that it would not contravene a business’s compliance with other privacy laws, such as the General Data Protection Regulation (GDPR) in Europe and consumer privacy laws recently passed in Colorado, Virginia, Connecticut, and Utah. In doing so, it simplifies compliance for businesses operating across jurisdictions and avoids unnecessary confusion for consumers who may not understand which laws apply to them.”).

August 22, 2022

Page 8

3. **Methods for Honoring Opt-Out Preferences Should Remain Flexible and Facilitate Consumer Choice as Intended by the CPRA (Section 7025).**

A. Proposed Modification

- (b) A business that elects to honor an opt-out preference signal pursuant to Civil Code section 1798.135(b) shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:
- (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.
 - (2) The platform, technology, or mechanism shall have the capability to clearly indicate the consumer's opt-out choice in a manner that complies with Section 7004, including accurately identifying the user as a California resident and disclosing any technical limitations of the mechanism.
 - ~~(3)~~ The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, ~~whether in its configuration or in disclosures to the public to the consumer that align with Section 7004~~, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information as defined under California law. ~~The configuration or disclosure does not need to be tailored only to California or to refer to California.~~
 - (4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business is not required to collect additional information to link the user to other accounts.
 - (5) The platform, technology, or mechanism that sends the opt-out preference signal shall have the capability to allow a consumer to clearly represent the consumer's intent and be free of defaults constraining or presupposing that intent.
 - (6) The platform, technology, or mechanism that sends the opt-out preference signal shall ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by a reasonable consumer.
 - (7) The platform, technology, or mechanism that sends the opt-out preference signal shall ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

August 22, 2022

Page 9

- (c) When a business that elects to honor an opt-out preference signal pursuant to Civil Code section 1798.135, subdivision (b) collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

...

- (3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business ~~shall process~~ may ignore the opt-out preference signal, if it notifies ~~but my notify~~ the consumer of the conflict and provides the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, or if the customer does not respond to the business within seven calendar days of receiving the notice from the business, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display, in a conspicuous manner, the status of the consumer's choice in accordance with section 7026, subsection (f)(4).
- (4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business ~~shall~~ may notify the consumer that processing the opt-out preference signal would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the consumer does not affirm their intent to withdraw, or if the customer does not respond to the business within seven calendar days of receiving the notice from the business, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display in a conspicuous manner the status of the consumer's choice in accordance with section 7026, subsection (f)(4).
- (5) A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

August 22, 2022

Page 10

- (6) The business ~~should~~may display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.
- (7) Illustrative examples follow.
- (A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled. Business N collects and shares Caleb's browser identifier for cross-contextual advertising, but Business N does not know Caleb's identity because he is not logged into his account. If Business N recognizes opt-out preference signals, upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.
- (B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu that recognizes opt-out preference signals. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.
- ...
- ~~(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to~~

August 22, 2022

Page 11

~~marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P’s website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal, but must notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.~~

~~...~~

- ~~(e) — Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or an alternate opt-out link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or an alternate opt-out link. It does not give the business the choice between posting the above referenced links or honoring opt-out preference signals. Even if the business posts the above referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above referenced links.~~
- ~~(f) — Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:~~
- ~~(1) — Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; or~~
 - ~~(2) — Change the consumer’s experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business’s product or service functions compared to a consumer who does not use an opt-out preference signal.~~
 - ~~(3) — Display a notification, pop up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. A~~

August 22, 2022

Page 12

~~business's display of whether or not the consumer visiting their website has opted out of the sale or sharing their personal information, as required by subsection (c)(2), shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) through (3).~~

- (~~eg~~) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or the alternative opt-out link. ~~if it meets all of the following additional requirements:~~
- ~~(1) Processes the opt out preference signal in a frictionless manner in accordance with the CCPA and these regulations.~~
 - ~~(2) Includes in its privacy policy the following information:~~
 - ~~(A) A description of the consumer's right to opt out of the sale or sharing of their personal information by the business;~~
 - ~~(B) A statement that the business processes opt out preference signals in a frictionless manner;~~
 - ~~(C) Information on how consumers can implement opt out preference signals for the business to process in frictionless manner;~~
 - ~~(D) Instructions for any other method by which the consumer may submit a request to opt out of sale/sharing.~~
 - ~~(3) Allows the opt out preference signal to fully effectuate the consumer's request to opt out of sale/sharing. For example, if the business sells or shares personal information offline and needs additional information that is not provided by the opt out preference signal in order to apply the request to opt out of sale/sharing to offline sales or sharing of personal information, then the business has not fully effectuated the consumer's request to opt out of sale/sharing. Illustrative examples follow.~~
 - ~~(A) Business Q collects consumers' online browsing history and shares it with third parties for cross contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set~~

August 22, 2022

Page 13

~~forth in Civil Code section 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.~~

~~(B) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1) and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.~~

B. Reasons for the Proposed Modification

We propose modifying section 7025 to align the regulation with the plain language of the CPRA statute, which creates flexibility for how businesses may honor opt-out of sale or sharing requests and ensures consumers make informed opt-out choices.

Initially, the Agency has exceeded its authority by directly contravening the CPRA statute and making it mandatory for businesses to honor opt-outs through both a "Do Not Sell or Share My Personal Information" link and opt-out preference signals. *See* Section 7025(e) ("Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner."). Under the CPRA, voters approved giving flexibility to businesses to not provide an opt-out link if they allow consumers to exercise their opt-out rights through a preference signal. *See* Cal. Civ. Code § 1798.135(b)(1). The Agency has contradicted this requirement by making it mandatory to honor opt-out preference signals, even if an opt-out link is provided, and by adding the caveat that, for businesses to only honor opt-out preference signals instead of providing the opt-out link, they must do so in a "frictionless manner," a term that is not substantiated in the CPRA and difficult to comply for businesses with a limited online presence.

Indeed, the Agency's draft regulation is also inconsistent with what was envisioned when drafting the CPRA. For example, when Alastair Mactaggart, Ashkan Soltani, and CalChamber's representative, Dominique Shelton Leipzig, were negotiating the opt-out preference signal requirements under the CPRA, the Global Privacy Control was developed as an alternative to the "Do Not Sell or Share My Personal Information" link to give flexibility for businesses. CalChamber members also had extensive discussions with Alastair Mactaggart where it was confirmed that the opt-out preference signal provisions were intentionally drafted to offer that

August 22, 2022

Page 14

option. The Agency has reduced this flexibility under section 7025, which CalChamber seeks to correct through the above modifications.

Next, not all businesses are alike and able to honor the same type of opt-out preference signals. We propose the modifications to section 7025(b) in the spirit of providing flexibility for businesses to address opt-out preference signals in a manner that is compatible with their technical abilities. For example, when a signal is an HTTP header field enabled through a browser extension, a business should not be required to collect additional information from a consumer in an attempt to link the signal to other accounts. Without such limitations, a business could unintentionally violate the rule merely because it did not receive the signal in a form that the business could process. This would be the same as holding a business liable for failing to honor an opt-out request sent to an email account that the business cannot access. The proposed modification is intended to avoid such a scenario. These revisions will help businesses with their already-onerous task of complying with the CPRA and avoid unintended consequences, because it will incentivize opt-out preference signal providers to develop alternative forms of signals to meet different technological capabilities of businesses.

Moreover, the proposed regulations should be amended to incorporate CPRA requirements for opt-out preference signals, such as being free of defaults that presuppose consumer intent, being clearly described and easy to use, and ensuring the opt-out signal does not conflict with other commonly used privacy settings. *See* Cal. Civ. Code § 1798.185(a)(19). The Agency should not ignore these statutory requirements and the complexity of implementing an opt-out choice preference signal. The Agency should also take a consistent approach to transparency and informed user choice in the context of opt-out preference signals and its implementation of other CPRA requirements. Accordingly, at a minimum, the provider of an opt-out preference signal should be required to disclose the limits of any signal, the potential conflicts with other privacy settings, and the specific definition of sale and sharing of data under the CPRA.

Additionally, the proposed regulations should permit businesses to honor consumers' business-specific privacy choices that conflict with an opt-out preference signal. Sections 7025(c)(3)–(4) address conflicts between a consumer's business-specific privacy settings and opt-out signals with a regulatory presumption that a consumer would choose the universal opt-out. This exceeds the spirit of the CPRA, which is premised on consumer choice and control, and supplants the Agency's choice for the consumers. Section 7025(c)(3) creates an overly burdensome requirement for businesses when consumer preference signals create conflicts. Businesses would either have to build new mechanisms that detect conflicts, honor the signal when a conflict is present, and then permit businesses to seek consent to re-enable choices that consumers have already made. This forces businesses to clear up the confusion created by the opt-out mechanism. As a result, the proposed regulations would effectively override the statutory specifications for the opt-out signals to notify consumers about the effect of the opt-out, creating even more confusion and degrading the consumer experience. The Agency's regulations should put consumers in control of their choices, not the Agency.

August 22, 2022

Page 15

4. The Proposed Requirements for Handling Opt-Outs of Sale and Sharing Should Be Revised To Limit Burdens on Businesses that Do Not Materially Benefit Consumers (Section 7026).

A. Proposed Modification

i. *Preferred Approach*

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it sells to or shares with third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online, the business ~~may shall, at a minimum,~~ allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the “Do Not Sell My Personal Information” link, the alternative opt-out link, or the business’s privacy policy.

...

(f) A business shall comply with a request to opt-out of sale/sharing by:

...

~~(2) Notifying all third parties to whom the business has sold or shared the consumer’s personal information, after the consumer submits the request to opt out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt out of sale/sharing and directing them to comply with the consumer’s request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

~~(3) Notifying all third parties to whom the business makes personal information available, including businesses authorized to collect personal information or controlling the collection of personal information on the business’s premises, that the consumer has made a request to opt out of sale/sharing and directing them 1) to comply with the consumer’s request and 2) to forward the request to any other person with whom the third party has~~

August 22, 2022

Page 16

~~disclosed or shared the personal information during that time period. In accordance with section 7052, subsection (a), those third parties and other persons shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.~~

~~(4) — Providing a means by which the consumer can confirm that their request to opt out of sale/sharing has been processed by the business. For example, the business may display on its website “Consumer Opted Out of Sale/Sharing” or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.~~

ii. *Alternative Approach*

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it sells to or shares with third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online, the business ~~may~~ *shall, at a minimum,* allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the “Do Not Sell My Personal Information” link, the alternative opt-out link, or the business’s privacy policy.

...

(f) A business shall comply with a request to opt-out of sale/sharing by:

...

~~(2) — Notifying all third parties to whom the business has sold or shared the consumer’s personal information, after the consumer submits the request to opt out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt out of sale/sharing and directing them to comply with the consumer’s request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

August 22, 2022

Page 17

- (23) Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises, that the consumer has made a request to opt-out of sale/sharing, and directing them ~~1)~~ to comply with the consumer's request unless such notification proves impossible or involves disproportionate effort and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period. In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.
- (34) Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website or its consumer privacy controls "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

B. Reasons for Modification

The proposed regulations could imply an interpretation that the regulations require businesses to apply opt-outs retroactively. The CPRA makes clear that opt-out requests apply only on a going-forward basis after the business receives the request from the consumer. *See* Cal. Civ. Code § 1798.120(d) ("A business that has received direction from a consumer not to sell or share the consumer's personal information. . . shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information *after its receipt of the consumer's direction.*") (emphasis added). As currently drafted, the regulations call into question whether an opt-out request must be conveyed to all third parties and limit use of previously sold or shared personal information. If the regulations were to be improperly interpreted to apply retroactively, this could involve a "disproportionate effort" as defined under draft regulation 7001(h). It would allow a consumer to revoke a business's previously received right to share or sell that consumer's personal information, instead of applying it on a going-forward basis. To comply, businesses would have to unwind prior data transactions to implement the opt-out requests across all downstream partners. This could be a complicated and burdensome process for businesses to ensure compliance, especially when dealing with third parties. Our proposed modifications address this issue by making clear that businesses need only apply opt-out requests on a going-forward basis as received. This change limits the burden on businesses. CPRA already requires notice of sharing or selling at the time of the collection of data; since the consumer had not elected to opt-out at the initial time of collection, the consumer knew and implicitly consented

August 22, 2022

Page 18

to the sale or sharing. For this reason, the business was well within its rights to share or sell the consumer's personal information.

In the alternative, if language on notice to third parties is retained, this section should be revised as proposed. This includes applying to only third parties to which a business has sold or shared a consumer's personal information and adding a disproportionate effort standard. We also have proposed deleting section 7026(f)(2), because the requirements appear entirely subsumed by 7026(f)(3), rendering it redundant.

Section 7026(f)(4) also requires a business to provide a means by which a consumer can confirm that the business has processed their opt-out request. This is a new requirement that extends beyond the statutory requirements. We recommend that, if a business is required to display a preference, it should have the option to show a preference within the privacy settings. A business should not be required to display a consumer's preference on the webpage, as this would unnecessarily clutter the user experience, be technologically difficult to implement, and may lead to confusion.

Finally, we propose modifications to section 7026(a) to align with the plain language of the CPRA statute that gives businesses the flexibility to honor opt-out of sale or sharing requests and ensures consumers make informed opt-out choices, as further described above.

5. Requirements To Prevent Dark Patterns Should Be Tailored To Address Fraudulent Practices Without Undermining Consumer Choice (Section 7004).

A. Proposed Modifications

- (a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.
 - (1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. ~~When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.~~
 - (2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be more burdensome or materially longer than the path to exercise a less privacy-protective option. Illustrative examples follow.
 - (A) A business's process for submitting a request to opt-out of sale/sharing shall not unreasonably require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out of sale/sharing is measured from

August 22, 2022

Page 19

when the consumer clicks on the “Do Not Sell or Share My Personal Information” link to completion of the request. ~~The number of steps for submitting a request to opt in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt in to completion of the request.~~

...

~~(C) — A website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, “Accept All” and “More Information,” or “Accept All” and “Preferences,” is not equal or symmetrical because the method allows the consumer to “Accept All” in one step, but requires the consumer to take additional steps to exercise their right to opt out of the sale or sharing of their personal information. An equal or symmetrical choice would be “Accept All” and “Decline All.”~~

~~(CD) A choice where the “yes” button is more prominent (i.e., materially larger in size ~~or in a more eye catching color~~) than the “no” button is not symmetrical, but colors can be used to aid the consumer’s choice (e.g., green for “yes” and red for “no”).~~

~~(DE) A choice where the option to participate in a financial incentive program is selected by default or featured more prominently (i.e., materially larger in size ~~or in a more eye catching color~~) than the choice not to participate in the program is neither equal nor symmetrical.~~

(1) Avoid language or interactive elements that are not clear and conspicuous and are intentionally confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer’s choice. ~~Illustrative example follows.~~

~~(A) — Giving the choice of “Yes” or “No” next to the statement “Do Not Sell or Share My Personal Information” is a double negative and a confusing choice for a consumer.~~

~~(B) — Toggles or buttons that state “on” or “off” may be confusing to a consumer and may require further clarifying language.~~

~~(C) — Unintuitive placement of buttons to confirm a consumer’s choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in~~

August 22, 2022

Page 20

~~the order of Yes, then No, but then offers choices in the opposite order—No, then Yes—when asking the consumer something that would benefit the business and/or contravene the consumer’s expectation.~~

- (1) Avoid manipulative language or choice architecture. The methods should not use language or wording that ~~guilts or shames~~ threatens or misleads the consumer into making a particular choice or bundles consent so as to subvert the consumer’s choice. Illustrative examples follow.
- (A) ~~When offering a financial incentive, pairing choices such as, “Yes” (to accept the financial incentive) with “No, I like paying full price” or “No, I don’t want to save money,” is manipulative and shaming.~~
- (~~A~~B) Requiring the consumer to click through false or misleading reasons why submitting a request to opt-out of sale/sharing is ~~allegedly~~ a bad choice before being able to execute their choice to opt-out is manipulative ~~and shaming~~.
- (~~B~~C) It is manipulative to bundle choices so that the consumer is only offered the option to consent to using personal information for reasonably expected purposes together with purposes that are incompatible to the context in which the personal information was collected. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer’s location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer’s geolocation to data brokers) together with the expected use of providing the location-based services, which does not require consent. This type of choice architecture is manipulative because the consumer is forced to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business’s use of personal information for ~~unexpected~~ ~~or~~ incompatible uses. By contrast, where the use of personal information is compatible with a requested good or service, the business need not offer a separate option. For example, using a consumer’s geolocation information to find the closest gas station is compatible with a mobile app that assists consumers in finding prices at local gas stations.
- (5) Easy to execute. The business shall not add unreasonable unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do

August 22, 2022

Page 21

not undermine the consumer's choice to submit the request. Illustrative examples follow.

(A) Upon clicking the “Do Not Sell or Share My Personal Information” link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

~~(B) Circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.~~

(B) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

B. Reasons for Proposed Modifications

Proposed section 7004(a) risks undermining consumer choice because the standards contained therein are ambiguous, subjective, and overly restrictive. It also contravenes the First Amendment protection allowing businesses to share truthful and accurate information with consumers. Our proposed modifications are not intended to undermine the purpose of section 7004, which is to ensure that consumers are presented with methods to submit rights requests and give consent without encountering “dark patterns.” Instead, we propose modifications to add reasonableness limitations and focus the requirements on design practices that give businesses the flexibility to adopt practical and appropriate methods, while not engaging in what can be fraudulent practices. These modifications are consistent with California's other consumer protection laws aimed to prevent fraudulent activities. *See, e.g.*, Cal. Bus. & Prof. Code § 17200 (defining unfair competition as including “unfair, untrue or misleading advertising”). Our modifications are also intended to give businesses flexibility to inform consumers regarding the implications of their decisions, such as the impact of opting out or choosing an option. Consumer choice is not meaningful if consumers' access to information is needlessly restricted. Accordingly, the Agency should revise the draft regulations to appropriately tailor the provisions targeting dark patterns.

Initially, section 7004(a)(2)'s requirement for symmetry should be based on a reasonable effort to achieve symmetry rather than having perfect symmetry. Perfect symmetry may not be possible in all contexts and could undermine consumer choice by restricting information or options. The illustrative example in section 7004(a)(2)(A), for instance, prohibits the process for submitting an opt-out request from involving more steps than a request to opt-in. However, there are instances where an additional step is necessary to provide a consumer with complete information about the impact of an opt-out request. As drafted, this extra step would be improper even if it is reasonable and likely helpful to consumers so that they can make informed decisions. To remedy this, we

August 22, 2022

Page 22

propose stating that businesses cannot “unreasonably” require additional steps. This will give businesses the opportunity to inform consumers regarding the disadvantages of opting out.

Similarly, section 7004(a)(2)(C) mandates an all-or-nothing approach for website banners that seek to allow consumers to exercise their rights. Yet, by limiting consumers to “accept all” or “deny all,” consumers cannot fully exercise their rights. A consumer may oppose the use of data for certain purposes and not others. The proposed regulation also does not allow consumers to exercise their rights in an informed manner, because it suggests that a “More Information” option is not permitted. This proposed regulation will not allow consumers to tailor consents based on their individual preferences. Thus, the Agency’s all-or-nothing approach for symmetry does not protect consumers. Rather, it deprives consumers of options and the information they would need to make informed decisions.

Further, the proposed modifications to section 7004(a)(3)-(4) are intended to prevent intentionally misleading designs, rather than strict requirements that may be unwieldy or unintentionally undermine consumer choice. Additionally, we suggest changes to focus on misleading or deceptive architecture. The First Amendment protects a business’s ability to share truthful and accurate information with consumers. *See, e.g., Central Hudson Gas & Electric v. Public Service Commission*, 447 U.S. 557 (1980). As written, section 7004(a)(4), in particular, could impinge on a business’s communication of truthful information about the effect of an opt-out request. Consumer choice is not informed if consumers’ access to information is needlessly restricted. Accordingly, the Agency should revise the draft regulations to appropriately tailor these provisions to address actual dark patterns, not restrict the flow of information.

Finally, we propose that section 7004(a)(5) be subject to a reasonableness standard to allow appropriate flexibility and avoid excessive penalization of businesses. The illustrative example in section 7004(a)(5)(B) demonstrates how this section could be applied in an overly burdensome manner. This example could be interpreted to mean that any broken link or nonfunctional email address creates liability, even though such failures happen despite robust practices to prevent them. These ordinary and isolated technical failures should not be the basis for liability. Adding a reasonableness standard (as opposed to one based on unnecessary burden or friction) remedies this issue.

6. Notice of Collection Requirements Should Be Reasonable To Avoid Becoming Cumbersome and Duplicative (Section 7012).

A. Proposed Modifications

i. *Preferred Approach*

(e) A business shall include the following in its notice at collection:

...

August 22, 2022

Page 23

- ~~(6) — If a business allows third parties to control the collection of personal information, the names of all the third parties; or, in the alternative, categories of the third parties' business practices.~~
- (f) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link ~~that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6) and includes headings to assist a consumer with finding this information. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.~~
- (g) Third Parties that Control the Collection of Personal Information. When more than one business may control the collection of a consumer's personal information, the businesses shall in a transparent manner determine their respective responsibilities for compliance with these regulations, which includes determining which business or businesses will provide notice at collection in accordance with the CCPA and these regulations. The businesses shall be accountable for their respective compliance with their designated responsibilities. This arrangement will appropriately reflect the respective roles and relationships of the businesses to consumers. The nature of the relationship shall be made available to consumers.
- ~~(1) — For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection.~~
- (1) This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subsection (f), and 7052, subsection (a).

August 22, 2022

Page 24

- ~~(2) — A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include in its notice at collection the names of all the third parties that the first party allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection.~~
- ~~(3) — A business that, acting as a third party, controls the collection of personal information on another business's premises, such as in a retail store or in a vehicle, shall also provide a notice at collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.~~
- ~~(4) — Illustrative examples follow.~~
- ~~(A) — Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.~~
- ~~(B) — Business H, a coffee shop, allows Business I, a business providing wi fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point of sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi fi services offered.~~
- ~~(C) — Business J, a car rental business, allows Business M to collect personal information from consumers within the vehicles Business K rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information~~

August 22, 2022

Page 25

~~about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.~~

ii. *Alternative Approach*

- (e) A business shall include the following in its notice at collection:

...

- (6) If a business allows third parties to control the collection of personal information, ~~the names of all the third parties; or, in the alternative, information about the categories of the third parties' the business allows to control the collection of personal information business practices.~~
- (f) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link ~~that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.~~
- (g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subsection (f), and 7052, subsection (a).
- (1) For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall

August 22, 2022

Page 26

provide a notice at collection. The third party may provide the notice at collection on its own webpage pursuant to Civil Code section 1798.100, subdivision (a) and need not provide the notice on the first party's website.

- (2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include, in its notice at collection, the categories of third parties with whom the first party names of all the third parties that the first party allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection. Whether the first party includes the third party's information in the first party's notice at collection will not affect the third party's obligations or compliance under this subsection.
- (3) A business that, acting as a third party, controls the collection of personal information on another business's premises, such as in a retail store or in a vehicle, shall also provide a notice at collection in a conspicuous manner, which takes into account the method of the data collection, at the physical location(s) where it is collecting the personal information.
- (4) Illustrative examples follow.
- ~~(A) Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.~~
- (AB) Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I

August 22, 2022

Page 27

shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.

- (~~BE~~) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.

B. Reasons for Proposed Modifications

We propose two options for modifying section 7012(e)-(g) to reduce confusion and unnecessary burdens that likely will result under the draft requirements.

Initially, the requirement in section 7012(f) that businesses link to specific sections of their privacy policy should be removed. This requirement will only result in businesses having to provide several different links to specific sections of the privacy policy to satisfy the notice at collection requirement. Allowing businesses to provide a link to their privacy policy that contains the required information and clear headers will allow for a less cumbersome consumer experience.

We also note that sections 7012(e) and (g) should be revised to better address the realities when multiple businesses control data collection to avoid multiple notices to consumers. As written, the section mandates duplicative disclosures and cumbersome mechanisms for these disclosures. More disclosures do not always benefit consumers as this can result in information overload or disclosures becoming white noise that consumers ignore. The benefit is further limited when consumers do not have a direct relationship with the third-party businesses providing notice.

Moreover, the draft regulations are contrary to the statutory text of the CPRA by requiring a list of third-party names. The CPRA only requires describing the *categories* of third parties, not their names. *See* Cal. Civ. Code §§ 1798.110(a)(4); 1798.115(a)(2); 1798.130(a)(3)(B)(ii); 1798.130(a)(4)(B). This requirement will also undermine the value of privacy policies by requiring lengthy and confusing language. The list of third-party names may have limited utility to consumers and impact the usability of the privacy policy. In fact, the requirement to provide a list of third parties in a business's privacy policy may conflict with confidentiality provisions in contracts. Indeed, some businesses guard the names of certain parties, such as data security providers, because this provides them with a competitive advantage. The proposed regulation will

August 22, 2022

Page 28

interfere with these businesses' ability to keep this information confidential without significantly bolstering consumers' rights.

Lastly, to achieve the purposes of the CPRA, only one party should provide notice that describes the categories of third parties with which personal information is shared. Our first proposed approach achieves this. This proposal also aligns the regulations with the GDPR, which allows joint controllers to "determine their respective responsibilities for compliance with" the GDPR, including the obligation to provide a privacy notice. *See* GDPR, Art. 26. If the Agency declines to adopt this proposal, we recommend that the Agency consider the second proposal. This alternative would at least mitigate issues related to disclosing names of all third parties and would adopt a reasonableness standard for notices provided at physical locations.

7. The Agency's Authority To Conduct Audits Should Be Subject to Reasonable Limits (Section 7304).

A. Proposed Modification

- (a) Scope. The Agency may audit a business, service provider, contractor, or person to determine compliance with any provision of the CCPA.
- (b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA if there are articulable facts leading to a reasonable belief that the business's collection or processing of personal information presents significant risk to consumer privacy or security. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.
- (c) Audits may be announced or unannounced as determined shall only be conducted upon no less than 60 days' notice by the Agency.
- (d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.
- (e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1997, Civil Code section 1798, et seq.
- (f) Prior to initiating an audit, the Agency must approve by majority vote a written order stating the scope of the audit. The audit may not exceed the scope of the written order and shall be limited to the CCPA provision or regulation that the Agency reasonably believes was or is being violated.

August 22, 2022

Page 29

(g) A business may request a hearing before an Administrative Law Judge to determine the propriety and scope of a written order commencing an audit.

B. Reasons for the Proposed Modification

Section 7304 should be modified to place reasonable limits on the conduct of Agency audits.

First, the proposal that the Agency may conduct audits to investigate possible violations without limits is unreasonable. Responding to audits can be incredibly burdensome for businesses to manage, even when a business has not violated the law. We encourage the Agency to exercise discretion in focusing audits on businesses where there are sufficient facts supporting a belief that a business's activities create a risk to consumer privacy or security in violation of the CCPA. This allows the Agency to use its resources in an efficient manner without burdening businesses with fishing expeditions. We have proposed modifications to align with this approach.

Second, the Agency's proposal that audits may be conducted without any advanced notice neither benefits the objectives of its investigations nor businesses. In advance of an audit, a business needs time to prepare so that it can provide an informed response to any inquiries by the Agency. A business will also need to coordinate with their privacy leaders and stakeholders to ensure their availability during the audit to provide responses to the Agency based on the actual practices of the business. For example, if there is an unannounced audit, the relevant persons within the business may be on vacation, traveling, or otherwise unavailable to provide appropriate answers to the auditors. As a result, the Agency may end up speaking to individuals within the business that do not have the relevant information, which may lead to a misunderstanding regarding the business's actual compliance with the CPRA. For this reason, we propose that the Agency provide at least 60 days' advance notice before conducting an audit so that the business has sufficient time to prepare and ensure the availability of appropriate persons to guide the Agency regarding the business's compliance program.

8. While Organizing Requirements for Service Provider and Contractor Agreements Is Valuable, Any Additional Requirements the Agency Is Seeking To Add Should Be Crafted To Benefit Consumers Without Unduly Burdening Businesses (Sections 7050, 7051, and 7053).

A. Proposed Modifications

i. *Section 7050*

- (a) A business that provides services to a person or organization that is not a business, ~~and that would otherwise meet the requirements and obligations of a "service provider" or "contractor" under the CCPA and these regulations, shall not be subject to the obligations of a "business" under be deemed a service provider or contractor with regard to that person or organization for purposes of the CCPA and~~

August 22, 2022

Page 30

these regulations with respect to its processing of personal information for that person or organization. However, such a business is not under an obligation to enter into a “service provider” or “contractor” agreement that complies with the CCPA and these regulations with the person or organization that is not a business. For example, a cloud service provider that provides services to a non-profit organization ~~and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall be considered a service provider even though it is providing services to a non-business~~ not be required to honor consumer rights requests under the CCPA and these regulations. The cloud service provider is also not obligated to be bound by contractual terms applicable for “service providers” or “contractors” under the CCPA and these regulations, because it is processing personal information for a non-business.

- (a) A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

...

- (2) For the ~~specific~~ business purpose(s) and service(s) set forth in, and in compliance with the written contract for services required by the CCPA and these regulations.

...

- (4) For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to directly perform services on behalf of another person. Illustrative examples follow.

- (A) An email marketing service provider can send emails on a business’s behalf using the business’s customer email list. The service provider could analyze those customers’ interactions with the marketing emails to develop or improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to directly send marketing emails on behalf of another business.

...

- (c) ~~A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising.~~ Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide

August 22, 2022

Page 31

advertising and marketing services, but those services shall not combine the personal information of consumers who have opted out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers. ~~A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor.~~ Illustrative examples follow.

- (1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses' websites, applications, or services identify users on the social media company's platform to serve advertisements to them.

ii. *Section 7051*

- (a) The contract required by the CCPA for service providers and contractors shall:

...

- (2) Include the required terms for such contracts under Civil Code 1798.100, subsection (d)(1). Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
- (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations. ~~This section shall~~

August 22, 2022

Page 32

~~list the specific business purpose(s) and service(s) identified in subsection (a)(2).~~

...

- (8) Require the service provider or contractor to notify the business ~~no later than five days~~ after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

...

- ~~(10) Require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider or contractor to comply with the request.~~

...

- ~~(e) A person who does not have a contract that complies with subsection (a) is not a “service provider” or a “contractor” under the CCPA. For example, a business’s disclosure of personal information to a person who does not have a contract that complies with these requirements may be considered a sale for which the business must provide the consumer with the right to opt out of sale/sharing.~~

...

- (de) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred, but the business never enforces the terms of the contract, ~~nor exercises its rights to assess, audit or test the service provider’s or contractor’s systems~~ it might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

iii. Section 7053

- (e) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the

August 22, 2022

Page 33

circumstances, where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred but the business never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

B. Reasons for Proposed Modifications

We appreciate the Agency organizing the provisions required for contracts with service providers and contractors in one location, considering that these requirements are distributed in different parts of the CPRA. However, as drafted, sections 7050 to 7053 will unduly burden businesses when contracting and overseeing service providers and contractors without providing benefits for consumers. We encourage the Agency to consider revising sections 7050 to 7053 to address these concerns.

First, we recommend modifying section 7050(a) to more directly address the purpose of this subsection per the Agency's Initial Statement of Reasons, which is to avoid "entities that process personal information on behalf of non-profit and government entities in accordance with a written contract [not to] be required to comply with consumer requests even when those nonprofits and government entities in ultimate control of the information are not required to do so." See [Initial Statement of Reasons](#) at 49. We have modified subsection (a) to make this point clear and to avoid other unintended effects of the Agency's proposed language, such as making a business acting as a service provider to a non-business (e.g., the State of California) implement a contract with the non-business that meets all of the terms of the CPRA and these regulations. This places undue and unintended burdens not only on service providers and contractors, but also on non-profits and governmental entities that are not within the scope of the CPRA.

Second, we recommend that section 7050(b)(4)(a) clarify that a service provider or contractor is still considered to be using personal information for internal purposes as long as it is not directly using the personal information to service another person. This is important because a service provider or contractor may generally improve its services based on personal information obtained from one business, which may benefit another person indirectly. This modification is necessary to draw that distinction and to avoid any unnecessary consequences of improving the services of service providers and contractors.

Third, we propose revising section 7050(c) to remove the verbiage regarding cross-context behavioral advertising and other restrictions. These issues are already dealt with in sufficient specificity in the statute. See Cal. Civ. Code § 1798.140(e)(6). Additionally, these restrictions are problematic, because they do not reflect that businesses that operate as service providers for one function may operate as a third party with respect to another function.

August 22, 2022

Page 34

Fourth, we propose modifying section 7051 to address overly prescriptive requirements for contracts that are not present in the CPRA statute. Under the proposed section 7051(a)(2), a business is required to “identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information.” This is a new requirement added by the Agency, which is not in the CPRA. The concept is carried over into proposed section 7051(a)(3) regarding various prohibitions, which also are to be tied to “the specific business purpose(s) and service(s) identified in subsection (a)(2).” This, too, is a new requirement added by the Agency and is not found in the CPRA. Small businesses, which may not even have internal legal staff to help write or review contracts, should not be placed in a position to violate the CCPA because their contracts do not contain specific listings of business purposes (a defined term under the CCPA) and services. As well, it will create an enormous burden on businesses that seek to prepare uniform data protection agreements as part of negotiating, in some instances, hundreds, if not thousands, of contracts with their service providers and contractors. The Agency should instead rely on the contract requirements already enumerated in CPRA for agreements between a business and its service provider, contractor, or third party. *See* Cal. Civ. Code § 1798.100(d)(1). The additional requirements in proposed section 7051 are overly prescriptive and do not further protect consumer privacy in any meaningful way. These provisions, which go beyond the plain text of the CPRA, also call into question the Economic Impact Statement released as part of this rulemaking. Any business would be hard-pressed to customize contracts as called for by these proposals while also limiting its *total* CPRA compliance costs to \$127.50 and increased labor requirements by 1.5 hours.

Fifth, we request that the Agency remove the five-business day deadline for a service provider or contractor to provide notice under section 7051(a)(8). This specific deadline is not included in the CPRA. *See* Cal. Civ. Code § 1798.100(d)(4). Businesses should be able to determine a deadline that makes sense based on their business and contract. Indeed, because of the Agency’s delay in publishing the draft CPRA regulations, many businesses have already begun the process of amending their contracts to address the new requirements for service providers and contractors based on the plain text of the CPRA statute. By including this additional requirement, businesses will have to redo these negotiations to address this unforeseen provision.

Sixth, we propose removing the section 7501(a)(10) requirement that contracts contain a provision obligating a business to inform a service provider or contractor of consumer requests. Businesses are unlikely to have this explicitly stated in existing agreements with service providers or contractors as there is no such requirement under the CPRA. As a result, these businesses may have to update many existing contracts to add this term. Mandating a contractual provision on this is unnecessary to achieve obligations under the CPRA.

Seventh, we propose removing section 7051(c) from the CPRA regulations because it is unnecessary. The CPRA statute already provides the requirement for there to be an agreement or written contract between the parties. *See* Cal. Civ. Code §§ 1798.100(d); 1798.140(j)(1); 1798.140(ag)(1). The effect of not having an agreement or written contract, but otherwise having

August 22, 2022

Page 35

a mutual understanding with your service provider or contractor, should be assessed on a case-by-case basis to see if it is truly a “sale” under the CPRA.

Lastly, as written, sections 7051(e) and 7053(e) potentially establish a requirement for businesses to conduct due diligence and audits of service providers, contractors, and third parties, even though there is no reason to believe that these parties are violating the CCPA or CPRA. The CPRA is clear that “the contract *may*, subject to agreement with the service provider, permit the business to monitor the service provider’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.” *See* Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added); *see also* Cal. Civ. Code § 1798.140(j)(1)(C) (permitting, but not requiring, audits). Thus, contrary to the plain text of the CPRA, the Agency is potentially making audits and diligence a mandatory requirement irrespective of the circumstances of the processing. Critically, requiring businesses to conduct audits and due diligence, even when there is no reason to suspect wrongdoing, will impose a significant burden on small businesses that do not have the resources to audit all of these suppliers on a routine basis. This will, in turn, divert resources that small businesses need for their general privacy compliance obligations. The proposed modification addresses this issue by requiring a business to know or have reason to know that there is a violation of the law before conducting diligence or an audit.

9. Notice Requirements in Connection with Phone Calls and Smart Devices Should Be Designed to Better Serve Both Consumer Privacy and the User Experience (Section 7013).

A. Proposed Modification

- (e) A business that sells or shares the personal information of consumers shall provide the notice of right to opt-out of sale/sharing to consumers as follows:

...

- (3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

...

- (B) A business that sells or shares personal information that it collects over the phone shall inform consumers of the notice and where it can be accessed ~~provide notice orally~~ during the call when the information is collected.

August 22, 2022

Page 36

- (C) A business that sells or shares personal information that it collects through a connected smart device (~~e.g., smart television or smart watch~~) shall provide notice in a manner that ensures that the consumer ~~will encounter~~ can access the notice while using the smart device.

...

- (h) A business shall not sell or share the personal information it collected after the effective date and during the time the business did not have a notice of right to opt-out of sale/sharing posted unless it obtains the consent of the consumer.

B. Reasons for the Proposed Modification

We have proposed a modification to section 7013(e) to ensure consumers can exercise choice by being able to determine the method for accessing the notice while contacting a business over the phone or using a smart device to better reflect how smart devices operate.

To foster consumer privacy, the emphasis in this section should be placed on whether a consumer can *access* the privacy notice during the call or while using the smart device, not whether they will *encounter* the notice on the smart device. Accessing the notice recognizes the importance of providing the consumer an opportunity to thoughtfully review the notice; conversely, merely encountering the notice does not ensure any meaningful opportunity to review and can interfere with the consumer's user experience on the smart device. For instance, a notice prompt on a smart watch every time a consumer opens a watch app would distract from the consumer's intended use of the smart device. In terms of telephone calls, consumers may not find it beneficial to listen to a notice of opt-out of sale/sharing and would prefer to read it themselves.

Lastly, section 7013(h) should apply to personal information collected after the notice requirement goes into effect under the CPRA. We propose modifications to this section to align this requirement.

10. **The Agency Should Accommodate the Possibility of Opt-In Consent for the Use of Sensitive Personal Information and Remove Excessively Restrictive Requirements That Do Not Materially Benefit Consumers (Sections 7014 and 7015).**

A. Proposed Modification

i. *Section 7014*

We propose inserting a new subsection (b) under section 7014 (with the subsections that follow the current subsection (a) renumbered) that will state the following:

August 22, 2022

Page 37

(b) A business is not obligated to provide a notice of right to limit if it obtains the consumer's explicit consent to process his or her sensitive personal information and, at the time of consent, discloses how the consumer may withdraw their consent in a manner consistent with the applicable provisions in sections 7003 and 7004.

ii. *Section 7015*

(b) A business that chooses to use an alternative opt-out link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon to the right or left of the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet homepages. ~~The icon shall be approximately the same size as any other icons used by the business on its webpage.~~

B. Reasons for the Proposed Modification

We recommend making minor modifications to sections 7014 and 7015 to provide both consumer choice and more flexibility to businesses.

First, we suggest that the regulations permit businesses to obtain opt-in consent *prior* to processing sensitive personal information for a purpose other than those enumerated in the statute, and provide consumers with a mechanism of withdrawing consent, in lieu of providing a notice of right to limit. This approach would be more privacy-protective by honoring consumer choice.

Second, as currently written, section 7015(b) would require an alternative opt-out link to be an icon that is the same size as other icons on a business's website. In effect, section 7015(b) could require opt-out links and icons to be the same size as the business's logo on its homepage. It also requires businesses to develop and define icons for each specific page on a website, which will require a different size icon for each page of a website. The burden of this requirement outweighs any value to the consumer. Thus, we recommend, at a minimum, removing the requirement that "[t]he icon shall be approximately the same size as any other icons used by the business on its webpage." This will help address this unintended consequence. The better and more consumer-friendly approach is to permit businesses to use a clearly labeled alternative opt-out link, such as when labeled "Your Privacy Choices." This will provide consumers with a clear link for reviewing and making privacy choices while giving businesses a straightforward and less burdensome way to develop a link across a single website.

August 22, 2022

Page 38

11. Requirements Related To Responding To Requests To Delete Should Be Reasonable To Achieve the Purposes of the CPRA Without Imposing Resource-Intensive Processes (Section 7022).

A. Proposed Modification

(b) A business shall comply with a consumer's request to delete their personal information by:

- (1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information;
- (2) Notifying the business's service providers or contractors to delete from their records the consumer's personal information obtained in the course of providing services; and
- (3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.~~

(c) A service provider or contractor shall, upon notification by the business, comply with the consumer's request to delete their personal information by:

...

- (4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If the service provider or contractor claims that such a notification is impossible or would involve disproportionate effort, the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort. The service provider or contractor shall not simply state that notifying those~~

August 22, 2022

Page 39

~~service providers, contractors, and/or third parties is impossible or would require disproportionate effort.~~

...

- (f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:
- (1) Provide to the consumer a ~~detailed~~ explanation of the basis for the denial, including any conflict with federal or state law, ~~or~~ exception to the CCPA, ~~or factual basis for contending that compliance would be impossible or involve disproportionate effort~~, unless prohibited from doing so by law;
 - (2) Delete the consumer's personal information that is not subject to the exception;
 - (3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and
 - (4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

B. Reasons for the Proposed Modification

We propose modifications to section 7022 to remove requirements for businesses, service providers, and contractors to provide consumers a detailed explanation regarding why deletion would be impossible or involve disproportionate effort.

As an initial matter, it is not uncommon for businesses to have hundreds, if not thousands, of service providers and contractors. If every consumer request to delete required a business to provide, or to receive from its service providers or contractors, a detailed explanation regarding why downstream notification would be impossible or involve disproportionate effect, the business would struggle to allocate sufficient resources and labor to handle its CPRA compliance efforts. Additionally, ensuring an accurate chain of communication to third parties may not be feasible in the digital marketplace. Similarly, as an operational matter, it is unreasonably burdensome to require a business to provide tailored and detailed explanations regarding the exemption it is relying on in denying a deletion request, in whole or in part. Critically, the Agency's proposed requirements for detailed explanations goes beyond the CPRA statute, which contains no such obligation. *See* Cal. Civ. Code § 1798.105.

August 22, 2022

Page 40

Thus, for these reasons, we request the Agency to limit section 7022 to what is required under the CPRA and adopt our proposed modifications.

12. The Proposed Requirement that a Business Notify Service Providers and Contractors of a Consumer’s Request To Correct Exceeds the Agency’s Authority Under the CPRA (Section 7023).

A. Proposed Modification

i. Preferred Approach

- (b) In determining the accuracy of the personal information that is the subject of a consumer’s request to correct, the business shall take commercially reasonable efforts to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information. ~~consider the totality of the circumstances relating to the contested personal information.~~ A business may deny a consumer’s request to correct if it determines that correction is not required under this subdivision ~~the contested personal information is more likely not accurate based on the totality of the circumstances.~~
- (1) For purposes of this subdivision “nature of the personal information and the purposes of the processing of the personal information” includes whether the information is or was factual.
- ~~(1) Considering the totality of the circumstances includes, but is not limited to, considering:~~
- ~~(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, e.g.).~~
- ~~(B) How the business obtained the contested information.~~
- ~~(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).~~
- (12) If the business is not the source of the personal information and has no documentation to support the accuracy of the information, the consumer’s assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

August 22, 2022

Page 41

- (c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected in its systems. ~~The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected.~~

...

- (f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~If the business denies a consumer's request to correct in whole or in part, the business shall do the following:~~

~~(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.~~

~~(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.~~

...

- (i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may~~shall~~^{749338220.2} provide the consumer with the name of the source from which the business received the alleged inaccurate information.

- ~~(j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).~~

August 22, 2022

Page 42

ii. *Alternative Approach*

- (c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected in its systems. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems unless such notification proves impossible or involves disproportionate effort. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected.

...

- (f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~If the business denies a consumer's request to correct in whole or in part, the business shall do the following:~~

~~(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.~~

~~(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.~~

...

- (i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business ~~shall~~ may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

...

- ~~(j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to~~

August 22, 2022

Page 43

~~allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).~~

B. Reasons for the Proposed Modification

To start, the Agency should strike the “totality of the circumstances” standard and related provisions from section 7023(b). This standard would create an onerous burden on a business’s legal department to get involved in each request to conduct this analysis. Instead, the Agency should align the standard for determining accuracy of information with other data protection laws, such as the GDPR, to facilitate a consistency compliance approach for businesses and consumers. *See, e.g.*, GDPR, Art. 5(1)(d). The Agency should also clarify that the scope of the request to correct under this section necessarily excludes inferences, probabilistic data, and marketing-related information generally.

As to section 7023(c), the Agency exceeds its authority by requiring a business to notify service providers and contractors of a consumer’s request to correct because there is no such requirement under the CPRA statute. Indeed, if the intent was to have such a requirement, it would have been included under the CPRA, as drafted in the right to delete. *Compare* Cal. Civ. Code § 1798.106 (no requirement to notify service providers and contractors), *with* Cal. Civ. Code § 1798.105(c)(1) (“A business that receives a verifiable consumer request from a consumer to delete the consumer’s personal information pursuant to subdivision (a) of this section shall delete the consumer’s personal information from its records, notify any service providers or contractors to delete the consumer’s personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer’s personal information unless this proves impossible or involves disproportionate effort.”). Alternatively, the Agency should adopt a more flexible standard that allows businesses not to provide notice to service providers or contractors if it would be impossible or require disproportionate effort. Our proposed modifications are important because section 7023 would impose significant operational burdens on businesses and require them to coordinate corrections with service providers and contractors in all instances, even when the processing of the personal information may not be germane to the business’s direct interactions with consumers.

Lastly, the Agency should delete section 7023(j). In addition to creating an operational burden on businesses, the regulation is duplicative of existing access and transparency requests in section 7024. We would also request the Agency to modify section 7023(f) as proposed, for the reasons explained under Section 7 of this letter.

August 22, 2022

Page 44

13. The Regulations Should Properly Place the Burden on the Consumer To Make a Specific Request for Information Exceeding the Prior 12 Months, Consistent with the Statute (Section 7024(h)).

A. Proposed Modifications

i. *Section 7024(h)*

- (h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022 or all the personal information it has collected and maintained about the consumer during the 12-month period preceding the business's receipt of the request. The business may provide all the personal information it has collected and maintained about the consumer on or after January 1, 2022 that is beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or, alternatively, the business shall notify the consumer that they can also request the personal information beyond the 12-month period preceding the business's receipt of the request. The information shall include any personal information that the business's service providers or contractors obtained as a result of providing services to the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer a ~~detailed~~ explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

B. Reasons for the Proposed Modification

The Agency should revise section 7024(h) to align with the allocation of responsibilities between the consumer and the business already provided under the CPRA. *See* Cal. Civ. Code § 1798.130(a)(2)(B). Under the statute, a consumer “may” request personal information beyond the 12-month period. However, the proposed regulations create ambiguity as to whether businesses are required to automatically provide personal information beyond the 12-month period by requiring that the business “shall” provide such personal information without specifying whether the consumer has requested this personal information. Also, the reference to January 1, 2022 in the statute was to make clear that there is no obligation to provide personal information collected prior to that time. But, under the text proposed, for a request received in December 2027 (as an example), the business would seemingly have to provide all information collected and maintained going back to January 1, 2022. The regulations should accurately allow businesses the flexibility to automatically provide the personal information beyond the 12-month period or to notify consumers of their ability to request personal information beyond the 12-month period upon

August 22, 2022

Page 45

the consumers' specific requests and also use the reference to January 1, 2022 for the purpose laid out in the statute.

14. The Regulations on Requests To Limit the Use or Disclosure of Sensitive Information Should Be Revised To Align with the Text of the CRPA Statute, Avoid Undermining Consumer Choice, and Support Efforts To Combat Crime (Section 7027).

A. Proposed Modification

(h) A business that uses or discloses sensitive personal information for the purpose of inferring characteristics creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (l).

(i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is more prominently also presented ~~than the other choices~~.

...

(l) The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes is not required to post a notice of right to limit.

...

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

B. Reasons for the Proposed Modification

Initially, we propose modifying section 7027(i), which requires that the single option be presented more prominently than other choices. Doing so would subvert consumer choice and unnecessarily

August 22, 2022

Page 46

impede the sharing of truthful and accurate information with consumers. In addition, adopting such a standard would contradict section 7004 by directing unreasonable asymmetry in choice architecture in this instance. The presentation of specific use cases/options for consumers should align with the same general choice architecture requirements otherwise proposed by the regulations.

Next, we recommend that the Agency remove from section 7027(1)(3) the limitation that the exception to the right to limit for malicious, deceptive, fraudulent, or illegal actions is only available when such actions are “directed at the business.” First, this language is predicated on the assumption that a business would be able to definitively know that such activities are directed at it. Instead, the Agency should promote transparency and working relationships with law enforcement agencies to stop bad acts, regardless of which business it is directed toward or whether it is possible to definitively tell. For example, if a business is aware that there is fraudulent activity directed at another business, the business should be permitted to use sensitive personal information to stop such activity and involve law enforcement if necessary. Limiting the ability of a business to disclose sensitive personal information in section 7027(1)(3) to only instances in which the business can tell that such acts are directed at it would impose unnecessary constraints, and potentially prevent businesses from proactively taking steps to stop crimes, even if possibly directed at other businesses.

15. Procedures for Probable Cause Proceedings Should Be Modified To Give Businesses an Opportunity To Respond To Allegations Before Initiating a Proceeding (Section 7302).

A. Proposed Modification

- (a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence sufficiently supports a reasonable belief that the CCPA has been violated.
- (b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.
- (c) Probable Cause Report. No probable cause proceeding will take place until at least 30 calendar days after the Enforcement Division provides the following, by service of process or registered or certified mail with return receipt requested, to each alleged violator:
 - (1) A probable cause report that contains a written summary of the law and evidence that supports the Agency’s reasonable belief that there is probable cause that each alleged violation of the CPRA has occurred, as well as a

August 22, 2022

Page 47

- description of any exculpatory evidence indicating a violation alleged in the report did not occur.
- (2) Notification that each alleged violator has the right to respond in writing to the Enforcement Division and the right to be present in person and represented by counsel at the probable cause proceeding.
- (d) Response to Probable Cause Report. Not later than 30 calendar days following service of the probable cause report, an alleged violator may submit to the Enforcement Division a written response to the probable cause report. The response should contain a summary of law and evidence that supports a position that the probable cause report fails to establish probable cause that any or all of the alleged violations of the CPRA occurred.
- (e) Probable Cause Proceeding.
- (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.
- (2) Agency staff shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and Enforcement Division staff shall have the right to participate at the proceeding. Agency staff shall determine whether there is probable cause based on the probable cause notice, probable cause report, and any information or arguments presented at the probable cause proceeding by the parties.
- (3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and Agency staff shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division.
- (f) Probable Cause Determination. Agency staff shall issue a written decision with their probable cause determination and serve it on the alleged violator electronically or by mail. ~~The Agency's probable cause determination is final and not subject to appeal.~~
- (g) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

August 22, 2022

Page 48

B. Reasons for the Proposed Modification

Section 7302 should be modified to provide businesses that are subject to a potential enforcement action an opportunity to receive all information that forms the basis of the alleged violations and be given an adequate opportunity to respond in writing in advance of the probable cause proceedings.

For example, the California Public Utilities Commission (CPUC) implements progressive enforcement, characterized as:

[A]n escalating series of actions, beginning with actions such as a warning letter or notification of violation followed by actions that compel compliance and may result in the imposition of penalties or fines (e.g., the issuance of an enforcement order or filing a civil or criminal action). Progressive enforcement may not be an appropriate enforcement response when violations result from intentional or grossly negligent misconduct, where the impacts on ratepayers or other consumers are widespread, or where impacts to safety are significant.

See CPUC Enforcement Policy, R. M-4846 at 4, (November 5, 2020). CPUC enforcement generally begins with a Notice of Violation, giving the entity 30 days to dispute or cure the violation. *Id.* at 8-9. There is the possibility to propose a negotiated settlement, to adopt an Administrative Consent Order, and to follow a Citation and Compliance Program. *Id.* at 10-12. And there is the possibility of an Order to Show Cause why a CPUC action should not be taken. *Id.* at 14.

The proposed modifications are intended to be consistent with this enforcement process and align with the CPRA statute, which requires the Agency to provide at least 30 days' notice before there is a finding of probable cause. *See* Cal. Civ. Code § 1798.199.50. The proposed modifications to section 7302 build on this process to develop a written briefing process in advance of the actual probable cause proceedings. This is also in line with the Fair Political Practices Commission (FPPC), which has a similar probable cause requirement, and includes a lengthy and detailed set of requirements on this point—including requiring a formal probable cause report, allowing for a written response and a reply, after which a probable cause hearing officer determines if there is probable cause to proceed.

Finally, we propose modifications to section 7302 to ensure that an alleged violator can receive detailed allegations and respond in advance of the hearing. We also propose a modification or an appeal right if there is an erroneous probable cause determination, which the current proposed draft does not allow. It is possible that the final determination was based on incorrect law or evidence, leading to further action against the business despite these errors. This proposal is intended to remedy this issue.

Mayer Brown LLP

August 22, 2022

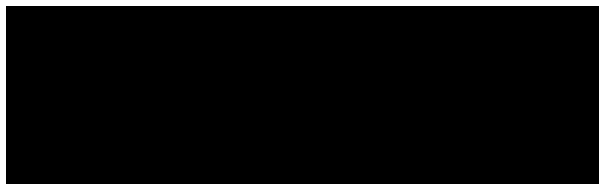
Page 49

In sum, with the above-proposed revisions, the Agency and businesses will have an opportunity to exchange critical information so that any decision regarding probable cause is fully informed and there is an opportunity to address any errors in the decision.

CONCLUSION

California voters entrusted the Agency with not only protecting personal information, but also ensuring a judicious balance between consumer privacy and business innovation. *See* Cal. Civ. Code § 1798.199.40(1). To ensure this balance, the CPRA grants the Agency a limited authority to enforce the CPRA consistent with its statutory provisions. *See* Cal. Civ. Code § 1798.199.40(b). Throughout this letter, we have identified a number of instances where the Agency has exceeded its authority or made proposals that create undue burdens for businesses without countervailing benefits for consumers. We request that the Agency consider our proposed modifications and ensure that the CPRA regulations align with the statute, as the voters intended.

Submitted on behalf of the California Chamber of Commerce



Dominique Shelton Leipzig,
Partner, Cybersecurity & Data Privacy
Leader, Global Data Innovation and Ad Tech Privacy & Data Management practices
Mayer Brown

Arsen Kourinian, Partner

Sasha Keck, Associate

Megan Von Borstel, Associate

Brittney Leyva, Associate

From: **Saunders, David P.** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 00:13:12 (+02:00)
Attachments: 8-22-22 CPPA Comment letter on behalf of MWE clients.pdf (8 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To Whom It May Concern,
Attached please find comments in response to the proposed CCPA regulations. Please do not hesitate to contact me with any questions or if you would like to discuss.

Best,
David

DAVID SAUNDERS (HE/HIM/HIS)
Partner
McDermott Will & Emery LLP 444 West Lake Street, Suite 4000, Chicago, IL 60606-0029

[REDACTED] | [REDACTED]

[Website](#) | [vCard](#) | [Twitter](#) | [LinkedIn](#)

Paul Cronin, Assistant to David Saunders

[REDACTED]

This message is a PRIVATE communication. This message and all attachments are a private communication sent by a law firm and may be confidential or protected by privilege. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the information contained in or attached to this message is strictly prohibited. Please notify the sender of the delivery error by replying to this message, and then delete it from your system. Our [Privacy Policy](#) explains how we may use your personal information or data and any personal information or data provided or made available to us. Thank you.

Please visit <http://www.mwe.com/> for more information about our Firm.



mwe.com

David Saunders
Attorney at Law

August 22, 2022

VIA EMAIL

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: Comments to Proposed California Consumer Privacy Act Regulations

Dear Board Members and Staff of the California Privacy Protection Agency:

McDermott Will & Emery appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency's (CPPA) July 8, 2022 Notice of Proposed Rulemaking under the California Privacy Rights Act of 2020 (CPRA). These comments are not provided on behalf of McDermott Will & Emery. Rather, we submit these comments on behalf of certain of our clients, who asked that we submit these comments on their behalf. These comments do not necessarily reflect the views of all of our clients. The clients for whom we submit these comments recognize the critical importance of individuals' privacy interests and the CPRA's protections, as well as the practical, business implications of California's privacy laws. These comments are meant to assist the CPPA in developing regulations that strike the best balance possible, both protecting the privacy rights of individuals and creating a practical implementation framework for businesses who provide valuable services to California residents.

Section 7012(f) - Requiring links to specific sections of a business' privacy policy

The proposed text of Section 7012(f) requires a business collecting information online to provide consumers with "a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6)." And further states that "[d]irecting the consumer to the beginning of the privacy policy...so that the consumer is required to scroll through other information...does not satisfy this standard." We anticipate significant implementation issues with this proposed regulation. We encourage the CPPA to amend this Section so as to require a link to *one* specific section of a business' privacy policy rather than what could be multiple different sections all at once.

**McDermott
Will & Emery**

444 West Lake Street Chicago IL 60606-0029 Tel +1 312 372 2000 Fax +1 312 984 7700
US practice conducted through McDermott Will & Emery LLP.

David Saunders
August 22, 2022
Page 2

Sections 7012(e)(1) through (6) require a business to provide notice of (1) the categories of personal information being collected; (2) the purpose for which the information is collected; (3) whether the information is sold or shared; (4) the length of time a business intends to retain the information; (5) if a business sells or shares the information, a link to the notice of the right to opt-out; and (6) if a business allows third parties to collect personal information, the names or information about those third parties' business practices. Privacy policies typically include each of these disclosures in their own section. For example, the industry standard for companies that are subject to the European Union's (EU) General Data Protection Regulation – and what EU regulators expect to see in privacy policies – is for there to be a specific section related to data retention. Similarly, post-enactment of the California Consumer Privacy Act (CCPA), it has become routine for businesses to have a “California Privacy Rights” or similar section in their respective privacy policies that contains, among other things, an opt-out link. It is also typical for online privacy policies to identify the purpose of collection and the listing of collected information in different sections. In short, because the content required by Sections 7012(e)(1) through (6) typically does not appear in a single location in a privacy policy, a single link cannot bring a consumer to each of those sections simultaneously, raising a practical implementation problem.

A regulation that prohibits making a consumer “scroll” while at the same time requiring links to multiple, “specific” sections of a privacy policy simply cannot be implemented as a practical matter. Perhaps the purpose of Section 7012(f) is to require companies to list all of the information in Sections 7012(e)(1) through (6) in a single place in a privacy policy, but doing so likely would result in a jumbled set of disclosures that consumers would find difficult to read. Additionally, collapsing multiple parts of a privacy policy into a single section may cause confusion amongst other regulators (e.g., EU data protection authorities) who expect to find information in separate sections.

Recommendation: We understand that CPPA's intent with Section 7012(f) as stated in its Initial Statement of Reasons (Reasons) is to “ensure that the consumer is taken directly to the information required by the notice and to prevent consumers being led on a wild goose chase for the material information.” Reasons at 18. However, we believe that the practical implementation issue we have identified requires addressing. Because the information identified in Sections 7012(e)(1) through (6) typically reside in different parts of a business' privacy policy, we recommend that the CPPA consider modifying Section 7012(f) to require a link to a specific part of a business' privacy policy rather than to multiple different parts.

Sections 7012(e)(6), (g) – Third party data collection

We have multiple concerns regarding the CPPA's proposed regulations regarding the disclosure of “Third Parties that Control the Collection of Personal Information,” and ask that the CPPA withdraw Sections 7012(e)(6) and 7012(g). In particular, the proposed regulations exceed the CPPA's jurisdiction – they are tantamount to an amendment to the CCPA itself. Even if the proposed regulations were within the CPPA's authority to promulgate, they will cause competitive harm to businesses and significant customer confusion.

David Saunders
 August 22, 2022
 Page 3

The CPPA recognizes in its Reasons that “[a]lthough Civil Code section 1798.100, subdivision (b), requires third parties controlling the collection to post the notice at collection on their website, consumers would never be able to learn what these third parties are doing with their information because they do not know where to look... In the alternative, the first party and third party can work together to include the required information in the first party’s notice at collection. This would address the need to identify the third party.” Reasons at 18. The CPPA Reasons lay bare the fact that the CPPA has decided, unilaterally, to alter the obligations imposed on third parties – and businesses – as set forth in the CPRA. The requirement that businesses specify – by name – the third parties with whom they share or sell information cannot be found anywhere in the text of the CPRA or original CCPA. If the CPPA believes that there is some gap in the statutory requirements, then that is an issue for the California legislature to take up, and not for the CPPA to legislate through regulation. Doing so would exceed the CPPA’s authority. *See* CAL. GOV. CODE § 11342.1 (“Each regulation adopted, to be effective, shall be within the scope of authority conferred and in accordance with the standards prescribed by other provisions of law.”); *Agnew v. State Bd. Of Equalization*, 981 P.2d 52, 59-60 (Cal. 1999) (“it is well established that the rulemaking power of an administrative agency does not permit the agency to exceed the scope of authority conferred on the agency by the Legislature.”); *Cal. School Bds. Ass’n v. State Bd. Of Educ.*, 113 Cal. Rptr. 3d 550, 566 (Cal. Ct. App. 2010) (“The scope or intent of a statute cannot be diminished or altered by a regulation purporting to interpret or implement it.”).

Beyond its lack of authority, the CPPA’s proposed regulations will harm businesses and consumers alike. As the CPPA is likely aware, business partnerships are highly sensitive, often governed by non-disclosure agreements to maintain competitive advantages. By requiring businesses to disclose their business partners, the CPPA is creating an environment in which businesses can easily discover the business partners of their competitors and take actions to reduce any competitive advantage. Requiring businesses to identify their business partners in a notice of collection will harm businesses.

In addition, the information required by proposed Sections 7012(e)(6) and (g) will serve little more than to confuse and lengthen privacy policies that consumers already find challenging to navigate.¹ Many businesses have relationships with multiple third parties. Section 7012(g)(2) would require that the business either identify each of these business partners – and thus expose the business to competitive harm as described above – or provide “information about [the Third Parties’] business practices” in its notice at collection. In the event that a business does the latter, an already lengthy privacy notice will now have paragraphs of additional text which explain not what the business’ practices are, but rather, the practices of a third party. This will only serve to lengthen privacy policies and confuse consumers who spend time reading about third party collection practices in the midst of a business’ own privacy notice.

Recommendation: Do not adopt proposed Sections 7012(e)(6) and (g).

¹ *See* <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>;
<https://www.commonsense.org/education/articles/its-not-you-privacy-policies-are-difficult-to-read/>;
<https://techcrunch.com/2019/06/13/privacy-policies-are-still-too-horrible-to-read-in-full/>

David Saunders
August 22, 2022
Page 4

Section 7004(a)(2) – Symmetry in choice

Our clients agree with the CPPA that businesses should offer transparent and equivalent privacy choices to consumers. However, Section 7004(a)(2) does not provide sufficient guidance to businesses on how to implement the requirements of Section 7004(a)(2). The illustrative examples are helpful in that they identify what the CPPA considers acceptable and not acceptable, but as the CPPA can appreciate, the possible language options presented to a consumer for privacy choices are virtually limitless. As a result, based on the text of Section 7004(a)(2) itself, businesses are left to guess as to whether the CPPA will agree that the language a business has chosen is symmetrical. A fully proscriptive model (e.g., a business must only offer a certain option or set of options) is not a sound pathway forward as it may not capture all of the different iterations of language that would be appropriate for consumer choice.

Recommendation: The CPPA should create a safe harbor set of what the CPPA views as symmetrical privacy choices. If a business elects to use an option from the safe harbor language, then it knows that it does not risk any enforcement action. If a business elects otherwise, then it has the remaining portions of Section 7004(a)(2) upon which to guide the language it uses when presenting options to customers. By creating a set of safe harbor consumer choices, the CPPA would significantly streamline its enforcement burden while providing much-needed regulatory certainty to businesses.

In addition to the above, we note an inconsistency in the application of Section 7024(a)(2)(A). That regulation provides that “[a] business’s process for submitting a request to opt-out of sale/sharing shall not require more steps than that business’s process for a consumer to opt-in to the sale of personal information after having previously opted out.” However, other portions of the proposed regulations permit opt-out requests to involve more steps. In the case of an opt-in, there is a single step: a request for the consumer to opt-in, to which the consumer can either agree or not. When a consumer elects to opt-out, as set forth in Section 7026(g), “a business may present the consumer with the choice to opt-out of the sale or sharing of personal information for certain uses” or for all uses. Similarly, pursuant to Section 7026(h), a business may respond to an opt-out request “by informing the consumer of a charge for the use of any product or service” as a result of the consumer’s opt-out choice. In these circumstances, the process for opting out will necessarily require more steps than the one-step opt-in process. We believe that there is an easy remedy to address this inconsistency.

Recommendation: Revise Section 7024(a)(2)(A) to provide that “a business’ process for submitting a request to opt-out of sale/sharing shall not require more steps than that business’s process for a consumer to opt-in to the sale of personal information after having previously opted out unless permitted by Section 7026.”

Section 7014(h) – Use of sensitive personal information

Section 7014(h) of the proposed regulations adds a new consent-based requirement that contradicts the rubric of CCPA and exceeds the CPPA’s jurisdiction. It states that “a business shall not use or disclose sensitive personal information it collected during the time the business did not have a notice of right to

David Saunders
 August 22, 2022
 Page 5

limit posted for purposes other than those specified in section 7027, subsection (1) unless it obtains the consent of the consumer.” This requirement is not found anywhere in the plain language of the CPRA. Rather, the CPRA requires businesses to allow consumers to limit the use of their sensitive personal information. CPRA largely is a notice-based regime, not a consent-based one; yet the proposed regulation would amend the law to add this consent provision.

For example, if a business collects sensitive personal information only for purposes permitted pursuant to Section 7027(1) and later decides that it wants to use the sensitive personal information for some other purpose, then the plain language of CPRA requires that the business update its privacy policy; and if that business then updates its privacy policy, it must provide notice to the consumer of the new use and opportunity to opt-out. At that point, if the consumer does not elect to opt-out, then under the plain language of CPRA, the new use would be permitted. Nothing in the CPRA requires the business to go to each and every one of its customers – potentially millions of consumers – and obtain their consent.

Recommendation: Revise Section 7014(h) so that it is consistent with the plain text of the CPRA and requires (1) revisions to a business’ privacy policy; (2) reasonable efforts to notify existing consumers of the new use and new opt-out right, including by, *e.g.*, emailing the consumers and describing the same; and (3) a delay in the implementation of the new use for a period of 30 days after notice to consumers.

Section 7023(i) – Source of purportedly incorrect information

Section 7023(i) of the proposed regulations provides that if a business is not the source of purportedly incorrect information about a consumer, the business “shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.” In the Reasons, the CPPA explained that the basis for this proposed regulation is to allow the consumer to then contact that party and request correction. *See* Reasons at 31. But what if a business does not know the source of the information? Often, businesses do not catalogue such information, and the best that they can offer is that the information came from a third party. Indeed, even if a business is cataloguing data sources, data may come from one source and then be modified by another. In short, there may not be a reliable method for informing the consumer as to the source and the cost and effort to comply with the CPPA’s proposed regulation will be enormous.

Recommendation: Modify Section 7023(i) to account for those situations in which the business cannot reliably identify the source of the data.

Section 7024(h) – Access to information

The proposed regulations require a business to provide “all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business’s receipt of the [access] request, unless doing so proves impossible or would involve disproportionate effort.” The draft language in the regulation, however, does not account for situations in which customers seek less information. In those instances where a consumer only wants

David Saunders
 August 22, 2022
 Page 6

their data for a specific period of time, the regulations should allow businesses to honor the consumer's request, rather than data-dump what could be years of information on the consumer.

Recommendation: Amend Section 7024(h) to provide “unless doing so proves impossible, would involve disproportionate effort, or where the consumer requests data for a specific time period.”

Section 7025 – Opt-out preference signals

The proposed regulations requiring businesses to comply with opt-out signals conflict with the express language of the CPRA, and the CPPA must not adopt them. In its Reasons, the CPPA has taken the position that it is a “misinterpretation” of the CPRA to conclude that “complying with an out-out preference signal is optional.” Reasons at 35. The CPPA is wrong.

CPRA Section 1798.135(b)(3) provides businesses with a choice: “a business that complies with [Cal. Civ. Code Section 1798.135(a)] **is not required to comply with** [Cal. Civ. Code Section 1798.135(b)]. For the purposes of clarity, a business **may elect whether to comply** with subdivision (a) or (b).” (emphasis added). There is no ambiguity in this provision. It creates a choice: businesses can either provide opt-out links *or* recognize an opt-out signal. Indeed, the language of 1798.135(b) starts, “A business shall not be required to comply with subdivision (a) **if** the business allows consumers to opt-out of the sale or sharing...through an opt out preference signal.” (emphasis added). If the CPPA's approach holds – that businesses *must* honor an opt-out signal – then the entirety of Cal. Civil Code Section 1798(a) is superfluous, an approach that no court would adopt. *See Wells v. One2One Learning Found.*, 141 P.3d 225, 248 (Cal. 2006) (recognizing “the principle of statutory construction that interpretations which render any part of a statute superfluous are to be avoided.”); *People v. Deleoz*, 296 Cal. Rptr. 3d 204, 218 (Cal. Ct. App. 2022) (recognizing that “one of the basic tenets of statutory interpretation” is avoiding a reading that renders parts of a statute superfluous).

In addition, the CPRA requires that the CPPA issue regulations that define the “technical specifications for an opt-out preference signal.” The draft regulations include a single sentence on this score, stating that “the signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.” Sec. 7025(b)(1). This technical “specification” is too generic to enable uniform compliance. The proposed regulations do not offer businesses any predictability as to the form or format of the opt-out signal that businesses are supposed to honor; and they offer no technological controls, no certification process, and no oversight. Quite literally, nothing prevents a technology company from developing what they call an opt-out signal, but that businesses attempting to comply with CPRA simply would not know to look for. This will create massive implementation challenges for businesses and lead to consumer confusion as to what is an effective opt-out signal. Additionally, the proposed regulations leave businesses in the untenable position of having to respond to a signal from any number of different technologies. If a business, acting in good faith, misses one, it nonetheless exposes itself to potential regulatory action. Particularly given the scope of these changes and the late date on which CPPA has developed these regulations, this would not be fair.

David Saunders
August 22, 2022
Page 7

Recommendation: Respect the express language of the CPRA and make clear that honoring opt-out signals is optional for businesses. In the alternative, the CPPA should develop a more robust set of technical requirements (*e.g.*, designating a single technology type to which businesses should be able to respond), or even a certification process for opt-out signal providers so that businesses have fair warning as to which technologies are approved. Better still, the CPPA could maintain a public list of which specific signals businesses will be responsible for recognizing.

Section 7025(c)(3), (4) – Conflicts between opt-out signal and consumer consent

As the CPPA recognizes in the Reasons, one of CPRA’s purposes is to allow consumers “meaningful control over businesses’ use” of their information. *See* Reasons at 7. The best and most clear way for consumers to do that is to provide their informed consent for a specific data use. If consumers have provided their consent, then that consent should take priority over any signal that a consumer may have enabled on their web browser and potentially forgotten was even active. Yet, Section 7025(c)(3) requires businesses to prioritize the mindless signal, and then reach back out to the consumer to inquire about the conflict. This makes the consumer privacy experience *more* cumbersome, not less, and overrides the express consent of a consumer. Similarly in 7025(c)(4), despite a consumer’s express opt-in decision to participate in a financial incentive program, the draft regulations would require a business to opt the consumer out from that same program and only after the fact, inform the consumer of that withdrawal. The effect could be that a consumer loses the benefit of the financial incentive (*e.g.*, misses the opportunity to obtain the benefit). Here again, the proposed regulations would harm consumers.

Recommendation: Where a business has obtained opt-in consent for, *e.g.*, participation in a financial incentive, the regulations should honor and prioritize that consent. If the CPPA will require businesses to honor opt-out signals, then when a business receives a signal that it can associate with a consumer who previously opted-in, the obligation should be for the business to have to check with the consumer to determine whether the consumer wants to opt-out. To do otherwise would undermine the express consent of the consumer and create a more burdensome privacy experience both for consumers and businesses.

Enforcement safe harbor

While businesses have had a year to prepare for the implementation of CPRA, our clients are seeking guidance from the CPPA as to when the proposed regulations will come into effect and the CPPA will begin enforcement. The proposed regulations include many obligations that are not contained in the plain language of the CPRA itself. As a result, businesses will need a period of time to implement the new requirements.

As the CPPA knows, Cal. Civil Code Section 1798.185(d) required adoption of final regulations by July 1, 2022. The purpose of that date was to give businesses at least 6 months within which to comply with the new regulations before CPRA and the regulations took effect. In contrast, it appears that CPPA will need several additional months, perhaps beyond January 1, 2023, to implement the regulations, leaving businesses with virtually no time to prepare. We ask that the CPPA make clear in its implementing

David Saunders
August 22, 2022
Page 8

regulations that either (a) the regulations will not take effect for at least a six month period or (b) the CPPA will not enforce the regulations until at least six months after they are finalized.

* * *

We hope that the CPPA finds these comments helpful. On behalf of our clients, thank you for the opportunity to comment on the proposed regulations.

Sincerely,



David Saunders

From: **Divya Sridhar** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 13:30:36 (+02:00)
Attachments: SIIA CPRA Comments 082322.pdf (13 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hi,

Please see attached for our public comments on the California Privacy Rights Act (CPRA) proposed rules.

We thank you for your time and consideration and are happy to meet to discuss further.

Best,
Divya



Divya Sridhar, Ph.D.

Senior Director, Data Policy

[REDACTED]
[REDACTED]

Siaa.net



August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Via email to regulations@coppa.ca.gov

Subject: California Privacy Rights Act (CPRA) Proposed Regulations (CPPA Public Comments)

Dear California Privacy Protection Agency:

On behalf of the Software & Information Industry Association (SIIA), we write in response to the CPPA's proposed rulemaking to implement the California Privacy Rights Act (CPRA) and update existing regulations under the California Consumer Privacy Act (CCPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We believe that data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of uniform data privacy practices. We have previously provided stakeholder input on CCPA and CPRA, as the law sets an important milestone for companies engaging in interstate commerce both within and outside of California.

We provide recommendations intended to better align the CPRA regulations with the letter and spirit of the statute. Our suggested edits to the proposed regulations are reflected in **green, bolded** text. We do so to avoid confusion across earlier drafts of the proposed regulations, including the edits in blue (new content) and red (content deletion to the draft).

- Recommendation 1: Modify the "average consumer" expectation for data collection to improve predictability, implementation, compliance, and enforcement. (§ 7002, § 7027 and § 7053)

- Recommendation 2: Clarify business implementation of the “right to limit the use of consumer’s sensitive personal information” and expectations with regard to consumers having to opt-in, which diverges from the original CCPA opt-out intent. (§ 7014 and § 7027)
- Recommendation 3: Streamline requirements for third parties to request notice at collection to reduce consent fatigue. (§ 7012)
- Recommendation 4: Clarify that recognition of the global privacy opt-out preference signal is voluntary. (§ 7025)
- Recommendation 5: Refine the expectations regarding when businesses must notify service providers and contractors about individual requests to correct and delete and update the definition of disproportionate effort to include other entities besides the business that may be enabling specific consumer requests. (§ 7023 and §7001)
- Recommendation 6: Refine language regarding the use of service provider and contractor data for product improvement. (§ 7050 (b)(4) and § 7050 (c)(2))
- Recommendation 7: Streamline requirements for third parties to fulfill consumer requests, in line with reasonable practices set forth by the business. (§ 7052)
- Recommendation 8: Reassess CPRA fiscal impact analysis to address new expectations.

Recommendation 1: Modify the “average consumer” expectation for data collection to improve predictability, implementation, compliance, and enforcement. (§ 7002, § 7027 and § 7053).

While we support the data minimization objectives of the CPRA, we are concerned that the proposed regulations’ reliance on an “average consumer” to guide businesses in data minimization and restrict the collection and use of personal information will lead to significant problems. First, the proposed requirement in § 7002 for businesses to only process data aligned to the expectations of the “average consumer” has no basis in the underlying statute (see Cal. Civ. Code § 1798.121) and does not have a recognized or consistent definition beyond the statute itself. Relying on this standard is likely to create uncertainty for consumers and businesses alike, lead to challenges for implementation, compliance, and enforcement, and not advance the data minimization objectives of the CPRA.

Second, this expectation hampers the business’s ability to process data for highly technical backend processes, such as product improvement, research, analytics, and the development of new products. Based on the proposed regulations, businesses will be required to seek a customer’s opt-in to conduct any form of these backend processes, if they are not on par with the average consumer’s expectations. This is especially problematic for small businesses that

are early in their product design phase. Businesses will face serious slowdowns in partaking in routine processes, such as running quality checks, developing comparisons to other products, conducting product upgrades, engaging in testing, and designing new features which are actually beneficial to consumers.

To remedy this, we suggest striking reference to the “average” consumer across the proposed regulations (as it appears in § 7002, § 7027 and § 7053), while incorporating further detail to clarify the expectations that need to be met. We also recommend updating the illustrative example to reflect that businesses can use consumer data (within the bounds of the data minimization principles) to support and improve existing products and to develop new products and services as long as they are pertinent to the same industry. The language (as-is) would serve as a critical barrier to innovation for nearly every sector.

We recommend the following change:

§ 7002. Restrictions on the Collection and Use of Personal Information.

(a) A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) (including present and future purposes) for which the personal information was collected or processed. To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing should must be consistent with what a an-average consumer would expect when the personal information was collected. A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer’s explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.

(b) Illustrative examples follow.

[...]

(2) Business B provides cloud storage services for consumers. An average consumer expects that the purpose for which the personal information is collected is to provide those cloud storage services. Business B may use the personal information uploaded by the consumer to improve the cloud storage services or similar services provided to and used by the consumer because it is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected. However, Business B should not use the personal information to research and develop unrelated or unexpected new products or services used for a different industry, such as a facial recognition service, without the consumer’s explicit consent because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. In addition, if a consumer deletes their account with Business B, Business B should not retain files the consumer stored in Business B’s cloud storage service because such retention is not reasonably necessary and proportionate to achieve the purpose of providing cloud storage services.

Recommendation 2: Clarify how a business implements the right to limit the use of consumer’s sensitive personal information and related expectations for consumer consent.

The CCPA was intentionally drafted to grant consumers the right to limit use of their personal information (including sensitive personal information) through opt-out processes. The statute requires businesses to provide a link with the “notice of the right to limit” to consumers. The proposed regulations conflict with this framework by requiring businesses to obtain consumers’ opt-in to process their sensitive personal information, unless they are using the information for a purpose designated in § 7027 (I), pg. 43. This goes well beyond the statutory framework (Cal. Civ. Code § 1798.121).

Likewise, sections § 7014 (Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link) and § 7028 (Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information) exceed the statutory requirements, by creating an opt-in consent framework aligned to § 7027 (I). In addition to the confusion it creates for businesses who have already built their “limit the use of my sensitive PI” link, the opt-in framework will lead to consent fatigue, which is the opposite of the original statutory intention: to allow customers more autonomy to limit the use of their data.

In order to refine this requirement and align it to the intent of the statute, we recommend referring to the list of permissible purposes in § 7027 (I) as “examples” and revising the interpretation of the statute to an opt-out framework. This will ensure businesses have flexibility in the types of uses of the data, including when working with service providers and other entities in the digital ecosystem. For example, in the regulations, explicit consent is required for use of geolocation data and sale and sharing of geolocation data in such a way that it would be cumbersome, if not impractical, for companies to conduct first party marketing of products/services. In particular, small businesses depend on sale and/or sharing of geolocation data to effectively market, advertise and provide products and services to employ their business model and generate revenue.

Indeed, the regulations include an exemption for businesses if the sensitive PI is used to “resist malicious, deceptive, fraudulent, or illegal actions *directed at the business*”. We suggest broadening this exemption to permit businesses to use sensitive PI in all first party efforts, not just those that are directed at the business. For example, a business may use information about a consumer’s ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech – activities that may not be directly related or negatively impact the business. Another example is a business’s use of sensitive data like geolocation information, which can be highly indicative of potential fraud.

We recommend the following change:

[§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.](#)

[...]

(l) **Examples of the** The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these **or related** purposes is not required to post a notice of right to limit.

(3) To resist malicious, deceptive, fraudulent, or illegal actions **directed at the business** and to prosecute those responsible for those actions, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose.

[...]

Add:

(8) Accomplish the purposes for which the business processes such data.

(9) To assist another covered entity, service provider, or third-party with a permissible use under this section.

Recommendation 3: Streamline notice at collection for third parties to reduce consent fatigue.

The proposed regulations would require first *and* third parties to give consumers notice at collection § 7012 (g)(1). This is problematic for numerous reasons. From an operational standpoint, this requirement creates an unnecessary obligation for businesses, which is not equally privacy protective. A single notice, by categories of parties of where data may be shared, should be sufficient. As written, the regulations will induce consent fatigue if every party in the data value chain requests consent, especially in instances where these parties may not have a direct relationship with the customer.

Second, the proposed regulations would require notification of the names of each third party permitted to collect personal information from the consumer (§ 7012(g)(2)). Businesses – including their subsidiaries, conglomerates, and other linked and shared identities – may engage in data sharing with a wide array of independent contractors and this requirement will be cost-prohibitive, onerous, and possibly risky. Disclosing the name of these entities could unintentionally be shared with and used by competitors that could lead to violating trade secrets. It will likely impose a disproportionate effort on businesses, without generating meaningful benefit to consumers and could raise competition-related concerns, all in the same stroke.

We recommend striking § 7012(g)(1) and § 7012(g)(2). Alternatively, we suggest incorporating clarifying language that exempts businesses that exert a disproportionate effort to comply from having to fulfill these requirements. We also recommend replacing the requirement that businesses disclose the “name” of third parties with the “category” that defines the third parties.

We recommend the following changes:

§ 7012. Notice at Collection of Personal Information.

(g) Third Parties that Control the Collection of Personal Information.

(1) For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection, **unless it involves a disproportionate effort.**

(2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include in its notice at collection the **categories names** of all the third parties that the first party allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection.

Recommendation 4: Clarify that recognition of the global privacy opt-out preference signal is voluntary.

The proposed regulations imply that opt-out preference signals are mandatory and, therefore, these signals are the *only* acceptable method to validate a consumer's right to opt out request. (Section § 7025) This goes beyond the statutory language (Cal. Civ. Code § 1798.135), which recommends a business provide two or more methods of interaction between the business and consumer to support opt-out requests.

This is of particular importance as we consider interactions where the customer may not have a direct relationship with the business that serves in other, indirect capacities, including that of a third party or contractor. It would be both impractical and not meaningful to expect a contractor to respond to an opt-out request from a consumer that it does not directly interact with on a regular basis.

The proposed edits would revise the provision to bring it in line with the way that the statute (Cal. Civ. Code § 1798.135) treats the recognition of global opt out preference signals (i.e., as voluntary instead of mandatory).

We recommend the following changes:

§ 7025. Opt-Out Preference Signals.

(b) A business **that elects to provide an opt-out preference signal pursuant to subdivision (b) of Section 1798.135** shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing

[...]

(c) When a business **that elects to provide an opt-out preference signal pursuant to subdivision (b) of Section 1798.135** collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 **— for that browser or device, and, if known, for the consumer.**

[...]

(3) If the opt-out preference signal conflicts with a consumer’s business-specific privacy setting that allows the business to sell or share their personal information, the business **shall process the opt out preference signal, but** may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer’s consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display in a conspicuous manner the status of the consumer’s choice in accordance with section 7026, subsection (f)(4).

[...]

(5) A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information, **unless the business obtains affirmative consent from the consumer.**

(6) The business **may should** display whether or not it has processed the consumer’s opt-out preference signal. For example, the business may display on its website “Opt-Out Preference Signal Honored” when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

[...]

(d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.

e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt out preference signals (2) providing the “Do Not Sell or Share My Personal Information” or (3) “Limit the Use of My Sensitive Personal Information” links or an alternate opt out link; or (2) processing opt out preference signals in a frictionless manner in accordance with these regulations and not having to

~~provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or an alternate opt out link. It does not give the business the choice between posting the above referenced links or honoring opt out preference signals. Even if the business posts the above referenced links, the business must still process opt out preference signals, though it may do so in a non frictionless manner. If a business processes opt out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above referenced links.~~

(f) (e) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:

(1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; or,

~~(2) Change the consumer’s experience with the product or service offered by the business. For example, the consumer who uses an opt out preference signal shall have the same experience with regard to how the business’s product or service functions compared to a consumer who does not use an opt out preference signal.~~

(2) (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content that unreasonably burdens a consumer in response to the opt-out preference signal. A business’s display of whether or not the consumer visiting their website has opted out of the sale or sharing their personal information, as required by subsection (c)(2), shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt out preference signal with respect to the business’s sale or sharing of the consumer’s personal information provided that it complies with subsections (f)(1) through (3).

[...]

(g) (f) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the “Do Not Sell or Share My Personal Information” link or the alternative opt-out link if it meets all of the following additional requirements:

Recommendation 5: Refine the expectations regarding businesses notifying service providers and contractors about individual requests to correct and delete.

The proposed regulations require the business to notify individual service providers and contractors that have previously received data when that data has been corrected, which extends beyond what is required in statute. This provision would impose a significant operational burden for companies, especially those that transferred data (to the service provider or contractor) a lengthy time frame prior to the correction request. Furthermore, a blanket

requirement like this doesn't take into consideration that individual data correction requests (e.g., voluntary change to a person's surname or address) may not be relevant to individual service providers or contractors that receive the data.

In practice, data requests to correct and delete may be automated processes, therefore the expectation that individual requests be communicated piecemeal to each service provider will hamper day-to-day data flows and operational processes undertaken by the business to carry out consumer requests – without providing tangible privacy protective benefits. The unintended result is that businesses will incur additional costs, with no practical gain to the consumer. There are also instances where this could harm anti-fraud efforts because this additional data may allow for bad actors to have additional information.

One way to eliminate this is to remove the requirement. Alternatively, the section could be revised to include robust exemptions for circumstances where the business or entities serving the business would expend a disproportionate effort to comply, which would make the environment for addressing the language in § 7023 f (2)¹ more feasible.

The regulations add a definition for “disproportionate effort” within the context of responding to certain consumer requests, like the request to delete in § 7022(c)(4). We recommend extending this definition of businesses' disproportionate effort to include other entities that serve on their behalf, including service providers, third parties, and contractors that use PI. We also recommend expanding the definition to include commercial purposes where there is disproportionate effort. The suggested extension (shown below) would be similar to § 7022(c)(4), where service providers *can* demonstrate disproportionate effort for requests to delete.

We recommend the following changes:

§ 7023. Requests to Correct.

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems, **unless it involves a disproportionate effort.** Service providers and contractors shall comply with the business's

¹ § 7023 (f) (2):

(f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:

(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.

instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected. Illustrative examples follow.

§ 7001. Definitions.

(h) “Disproportionate effort” within the context of a business responding to a consumer request, or service provider, third party, contractor, or other entity serving or enabling the business in response to a request, means the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request. For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and would not impact the consumer in any material manner. In contrast, the benefit to the consumer of responding to a request to correct inaccurate information that the business uses and/or sells may be high because it could have a material impact on the consumer, such as the denial of services or opportunities. Accordingly, in order for the business to claim “disproportionate effort,” the business would have to demonstrate that the time and/or resources needed to correct the information, or the time and resources expended communicating with a service provider, contractor, or third party to correct the information, would be significantly higher than that material impact on the consumer. A business that has failed to put in place adequate processes and procedures to comply with consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort.

Recommendation 6: Clarify text about the uses of service provider and contractor data for product improvement in article 4, § 7050 (b) (4) and service provider data processing for cross-contextual advertising in § 7050 (c)(2).

The proposed regulations include revised language that makes the operational implications of how service providers and contractors use data unclear, for the purposes of 1) new product development and 2) for first party advertising using email addresses.

First, the proposed regulations would impose restrictions on these entities’ use of data to build new products and services within the service provider’s own product line, vertical, and/or industry. The regulations should lift these restrictions on service providers, so they can use consumer data to support new product and service lines. Second, the example in § 7050(c)(2) signals that businesses would be prohibited from any form of first party advertising based on email addresses.

The proposed regulations should be revised to ensure flexibility for service providers and contractors to use personal information to support new products and services within their vertical, and also to ensure that they can proceed with first party, tailored advertising using consumers’ personal information, such as email addresses. Businesses, service providers and contractors will be subject to compliance with these policies in at least five states in the coming months, and a streamlined approach to business, service provider, and contractor use of

personal information for targeted advertising will alleviate compliance hurdles and confusion across the business and consumer community.

We recommend the following changes:

§ 7050. ~~§ 7051.~~ Service Providers and Contractors.

(b) ~~(e)~~ A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

~~(4) (3)~~ For internal use by the service provider or contractor to build or improve the quality of its **present and future products and** services, provided that the service provider or contractor **does not use the personal information to perform services on behalf of another person business** ~~include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;~~ Illustrative examples follow.

(A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

[...]

(c) A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor.

Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). **The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business**

S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses's websites, applications, or services. ~~identify users on the social media company's platform to serve advertisements to them.~~

(2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

Recommendation 7: Streamline requirements for vendor contracts to reduce redundancy in expectations to notify vendors of individual consumer requests.

While we commend the intent of the CPPA for adding clarity to the roles and responsibilities of the businesses and third parties in the data value chain, we recommend streamlining the section so that businesses will not have to undertake significant and disproportionate effort to comply with a deluge of complex new requirements that may not be critical or time sensitive. For example, requirements for third parties to comply with consumer requests should be aligned with the business' schedule and timeframe for completing such requests so that the business is not required to individually contact third parties for each consumer request.

As noted in Issue 5, practices taken by the business and its respective service providers, contractors and third parties are regularly automated, therefore additional flexibility to the business will allow for these requests to be handled uniformly, without imposing a disproportionate effort on the business to carry out these changes. This will also further mitigate confusion when contractors, subcontractors and third parties are located in unique geographic regions and it may be difficult to honor unique data retention schedules and requirements.

We suggest the following change:

§ 7052. Third Parties.

(a) A third party shall comply with a consumer's request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information. The third party shall comply with the request, **in accordance with the business and its respective schedule and data retention practices to fulfill requests,** in the same way a business is required to comply with the request under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations.

Recommendation 8: Reassess CPRA fiscal impact analysis to address new expectations.

After a thorough analysis of the proposed regulations and their divergence from the statute, it seems likely that the estimated cost of compliance for businesses appears to materially understate the actual costs that businesses will incur.

The CPPA's Economic and Fiscal Impact Statement² estimates that 66,076 businesses will incur an additional \$127.50 per business to comply with the changes proposed in the rulemaking, which the CPPA estimates will require an additional 1.5 hours of work for each affected firm. We believe this estimate and underlying calculations³ significantly underestimates the actual cost for firms to comply with the new regulations.

As noted, after reviewing the draft regulations, we have identified numerous areas where the regulations significantly diverge from the statute – due to the addition of new privacy requirements and expectations of businesses, service providers, and other affected entities – which will likely further impact the bottom lines of companies scrambling to comply. We believe that the draft regulations should be further clarified and aligned to the statute, so that companies are not left with additional outstanding questions, onerous requirements that result in negligible privacy protective benefits to consumers, and high costs to comply, as the CPRA goes into effect on January 1, 2023.

Also of note, the estimate assumes that businesses that are now working to conform to CPRA are already in compliance with the most recent changes to the CCPA. This may overstate the preparedness of most businesses and their expected fiscal outlay for privacy compliance. We urge the CPPA to request additional stakeholder feedback in order to demonstrate these calculations and assumptions more accurately.

* * *

Thank you for considering our suggested revisions to the proposed regulations to the CPRA. We are happy to discuss in further detail, as appropriate. For further information, please contact Divya Sridhar, at [REDACTED].

Respectfully submitted,

Divya Sridhar, Ph.D., Senior Director, Data Policy
Software and Information Industry Association (SIIA)

² CPPA. [Economic and Fiscal Impact Statement](#). July 8, 2022.

³ California Consumer Privacy Agency. [Notes on Economic Impact Estimates for Form 399](#), June 27, 2022.

From: **Pregel, Katherine** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment: CPRA Proposed Regulations
Date: 23.08.2022 14:59:44 (+02:00)
Attachments: Labcorp Comments to CPPA Proposed CPRA Regs.pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,

Please accept the attached comments of Laboratory Corporation of America Holdings (Labcorp) on the proposed rulemaking to adopt regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA) issued by the California Privacy Protection Agency (CPPA) on July 8, 2022.

Please let us know if you have any questions.

Thank you,
Katherine Pregel



Katherine Pregel
Director, Government Relations & Public Policy
Laboratory Corporation of America Holdings

[REDACTED]
Office: [REDACTED]
Email: [REDACTED]

-This e-mail and any attachments may contain CONFIDENTIAL information, including PROTECTED HEALTH INFORMATION, and is meant to be viewed solely by the intended recipient. If you are not the intended recipient, any use or disclosure of this information is STRICTLY PROHIBITED; you are requested to delete this e-mail and any attachments and notify the sender immediately.



Laboratory Corporation of America® Holdings
531 South Spring Street
Burlington, North Carolina 27215

Katherine Pregel
Director, Government Relations & Public Policy
Telephone: [REDACTED]
Email: [REDACTED]

August 23, 2022

Via E-Mail: regulations@cpha.ca.gov

The California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: CPPA Public Comment: CPRA Proposed Regulations

Dear Mr. Soublet:

Please accept these comments of Laboratory Corporation of America Holdings (Labcorp or the Company) on the proposed rulemaking to adopt regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA or the Act) issued by the California Privacy Protection Agency (CPPA) on July 8, 2022. Labcorp is a leading global life sciences company headquartered in Burlington, North Carolina that provides vital information to help doctors, hospitals, pharmaceutical companies, researchers, and patients make clear and confident decisions. Through our unparalleled diagnostics and drug development capabilities, we provide insights and accelerate innovations to improve health and improve lives. Of our 75,000 global employees, over 4,200 Labcorp employees work in multiple facilities in California, providing clinical laboratory and drug development services to California residents and businesses. Labcorp would be directly affected by the proposed regulations.

I. Background

On July 8, 2022, the CPPA commenced the formal rulemaking process to adopt regulations to implement the CPRA. The proposed regulations: (1) update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; (2) operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the

law; and (3) reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand.

II. Specific Comments

Our comments on specific sections of the proposed regulations are provided below:

A. Section 7002(b)(2).

The illustrative example of Business B given in Section 7002(b)(2) appears to treat processing of personal data by a business for all “unrelated” product research and development as a necessarily incompatible purpose for which separate consent is always required. We consider this to be an overly restrictive interpretation of what is “incompatible” that is not supported by the Act and that risks impairing the ability to conduct important research and development. While some processing for research (such as the example given, creating an unrelated facial recognition product) would be incompatible, there are many instances where use of personal information for new product development would not be incompatible with reasonable consumer expectations and would cause no harm to the consumer. For example, these instances may include:

(i) looking at specific use cases (and the associated personal information) to analyze issues or problems with an existing product with a view to creating a new product that avoids such problems, even if such new product serves a different market or has a different purpose; and

(ii) developing aggregate data and statistics based on personal information to assess trends and needs for new products.

Such uses are generally permitted for service providers under Section 7050(b)(4) of the proposed regulations, which permits use of personal information for “internal use by the service provider or contractor to build or improve the quality of its services...”. This concept is also captured in the CCPA’s definition of “business purposes” to include “Undertaking internal research for technological development and demonstration” as described in Cal. Civil Code 1798.140(e)(7).

For these reasons, we suggest narrowing the Business B example so that it applies only to the facial recognition product scenario described.

B. Section 7003.

There is a conflict between the requirement to use “plain, straightforward language and avoid technical or legal jargon” set forth in Section 7003 and certain requirements set forth elsewhere in the proposed regulations. Section 7011(e)(1)(A), for example, requires use in the Privacy Policy of the “specific terms” from CA Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (9), which include such non-consumer friendly formulations as “Any personal information described in subdivision (e) of Section 1798.80” and “Characteristics of protected classifications under California or federal law.” Section 7003 should make it clear that the requirement to use plain language is subject to the need otherwise to comply with the specific requirements of the CCPA and the Regulations, even when those requirements require technical language.

Thank you for your consideration of Labcorp’s comments on CPPA’s proposed regulations to implement the CPRA.

Very truly yours,



Katherine Pregel
Director, Government Relations & Public Policy

From: **Shanahan, Richard** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Tolentino, Melissa** [REDACTED]
Subject: Comments for NPR on Updates to CCPA
Date: 23.08.2022 15:30:39 (+02:00)
Attachments: 08232022_CCPA Comments.pdf (4 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency Board:

Please find attached comments from Hitachi Group Companies doing business in the U.S. on the recently announced rulemaking for updates to the California Privacy law.

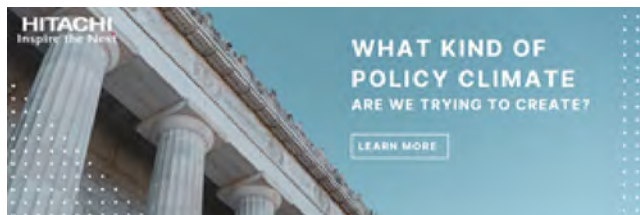
If you have any questions, please let us know.

Best regards,

Richard Shanahan

Director | Government & External Relations
Hitachi, Ltd. | Washington, DC Corporate Office

t. [REDACTED] | m. [REDACTED]
[REDACTED]



August 23, 2022

The Honorable Jennifer Urban, Chair
California Privacy Protection Agency board
2101 Arena Blvd.
Sacramento, CA 95834

RE: Notice of Proposed Rulemaking Concerning Updates to the California Consumer Privacy Act Regulations

Dear Chair Urban:

The following comments are submitted by Hitachi Group companies (“Hitachi”) doing business in the United States in connection with the Notice of Proposed Rulemaking Action (NOPA) *to amend and repeal portions of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA)*.

Background on Hitachi

Founded in 1910 and headquartered in Tokyo, Japan, Hitachi, Ltd. is a global technology corporation answering society’s most pressing challenges through cutting-edge operational technology (OT), information technology (IT), and products/systems. A Social Innovation leader, Hitachi delivers advanced technology solutions in the mobility, human life, industry, energy, and IT sectors. The company’s consolidated revenues for FY2021 (ended March 31, 2022) totaled \$84.13 billion and 853 companies employ over 368,000 employees worldwide.

Since establishing a regional subsidiary in the United States in 1959, Hitachi has been a committed American partner. For over thirty years, it has invested heavily in research and development (R&D) in the U.S., and this continued reinvestment has resulted in 19 major R&D centers that support high-skilled jobs in manufacturing and technology. Dedicated to delivering the technologies of tomorrow, Hitachi opened a Center for Innovation in Santa Clara, California to explore applications in machine learning, artificial intelligence, Internet of Things (IoT) devices, data analytics, and autonomous vehicles among other advanced technologies. Hitachi is also proud of its human capital investment with more than 25,000 employees across 81 companies in the U.S. At 15% of total revenue, North America is Hitachi, Ltd.’s second largest market, following only the Japanese market, with \$12.7 billion in revenue in FY2021.

Hitachi continues to appreciate the opportunity to engage with the Board and for the ability to offer comments and reactions to proposed changes. Privacy standards should be fair, equitable, and protect the public while also fostering innovation in the State of California and across the country.

Hitachi’s Approach to Privacy

Hitachi aims to co-create a human-centric society in which everyone can enjoy the benefits of digital technologies, and customer and employee privacy is central to that vision. Towards that end, we have developed and implemented a privacy-review process that includes regular, company-wide evaluations to identify insufficient practices, action plans to bolster privacy protections, and rigorous audits to ensure continuing compliance.

We also use privacy-focused training programs to make sure our critical, decision-making employees stay up-to-date on the company’s latest privacy requirements. By prioritizing privacy education in this manner, we ensure that privacy dictates our employees’ decision-making process around all forms of data. Our

Information Security Risk Management Division continuously monitors changes to privacy laws across countries.

Given Hitachi's global footprint and diverse business interests, consistent privacy regulations across federal and international borders are paramount to fostering the privacy ecosystem. At present, we adhere to GDPR and the Illinois Biometric Act, and we encourage CCPA to harmonize with these, federal statutes that have already been enacted for specific segments of the population or industries, and new state laws in Colorado, Connecticut, Utah and Virginia. At Hitachi, we believe it is imperative that we not only comply with applicable laws but also cultivate an environment of trust and privacy by design.

Responses to NOPA

Business Threshold Requirements (Civil Code Section 1798.140, subdivision (c))

In Hitachi's December 2019 comment letter to the California Attorney General, we noted concerns on the threshold questions for business in the state. The current definition of \$25M in gross revenues does not clarify where that revenue is to be derived from, which causes confusion. It would be helpful for CCPA to adopt a new clarification similar to other states in an effort to provide harmonization:

(c) "Business" means:

- (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
 - (A) produces a product or service that is targeted to consumers who are residents of the state;
 - (B) has annual revenue of \$25,000,000 or more, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.115; and
 - (C) satisfies one or more of the following thresholds:
 - (i) during a calendar year, controls or processes personal data of 50,000 or more consumers; or
 - (ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 50,000 or more consumers.

Definitions

Hitachi appreciates the changes to "Authorized agent." While the original scope was narrow, global businesses may not be registered in a particular state or country. By broadening the definition, consumers have more choices as to who can act on their behalf.

CCPA has added a new term, "Disproportionate Effort," which seems to provide businesses some guidance for determining the response to a consumer and potentially eliminating time-consuming requests. The definition, however, creates a new burden, and it is unclear what the threshold is. A consumer, or CCPA, may come to a different conclusion than the business after performing complex calculations. The end of this definition appears to state that a business that fails to create a process to determine disproportionate effect cannot use this as a rationale for avoiding compliance to a request, but does not state that the business is free from liability if it has a process even if different conclusions are met. Hitachi recommends that CCPA add more descriptive text to this definition and specifically allow for a safe harbor for businesses who create and apply reasonable processes.

Hitachi noted the ambiguity around the “Household” definition in our 2019 filing. We appreciate CCPA also seeing this definition as problematic and eliminating it.

Restrictions on the Collection and Use of Personal Information

Section 7002 provides information on considerations for a business when obtaining consumer information. In example (b)(4), the regulations describe a situation in which Business D transmits delivery information to Business E for the purpose of shipping a product to a consumer. The example notes the transfer by Business D to E is acceptable for Business E to use that data for delivery, but Business E cannot use the consumer information for marketing of another business’ products or for activities that are incompatible with the consumer’s expectation of Business E’s use of consumer data.

While appreciated, the example leaves out how to treat consumer information if Business E uses another business as part of its delivery optimization process. Here, Business E could contract with another company to help optimize the delivery routes and/or schedules to make the system more efficient. In this scenario, would the transfer of information collected by Business D, transmitted to Business E for delivery and then transferred it to an additional company for route optimization, be a permitted action under the regulations?

Verification of Requests

Article 3 lays out various considerations businesses can consider when verifying a request to “Know, Delete, Opt-Out, and Opt-In After Opting-Out.” The regulations, however, create gaps that do not provide certainty on liability issues such as the following:

1. If a business employs a “reasonable method” for verifying a request, is the business protected from liability if the request turns out to be fallacious?
2. If a business declines to fulfill a request because it has a good-faith belief the requestor is not verified, or if there is not enough information to reasonably verify the requestor, is the business held harmless if it turns out the request did come from a valid requestor?

Concerningly, some businesses could avoid California as a commercial market or move cutting-edge research out of the state to avoid unnecessary liability if there are not clear safe harbor provisions when a company puts into place reasonable, risk-based verification methods as generally outlined in Article 3. Small businesses in particular could find these verification methods particularly onerous. Given that, the Board should recognize a business’s resources and capabilities when determining if the business has created a reasonable standard for verification.

In lieu of creating prescriptive rules regarding verification, Hitachi recommends that the Board create a guidance document that favors a risk-based verification process and also considers the sensitivity of the data that is being processed. The regulations could then cite adherence to the guidance document as part of a test to create a safe harbor provision for businesses under this verification title. This would allow some flexibility as technology and security advance, and would give businesses certainty to liability under the title.

Business Outside of CA

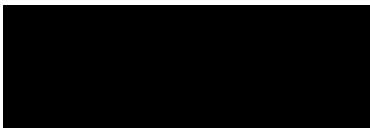
We noted in previous filings concern with how business activities outside of California are treated; this continues to be a concern. California Civil Code 1798.145(a)(6) states that the statute will not restrict a business’ ability to “collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California.” While clarifying language states “commercial conduct takes place wholly outside California if the business collected that information while the consumer was outside California, no part of the sale of the consumer’s personal information occurred in California, and

no personal information collected while the consumer was in California is sold,” this adds complexity as to exactly when a potential consumer was physically in the state. If a California resident is not physically in California when data is collected, is that information exempt from CCPA? Other portions of the regulations seem to intimate that merely being “domiciled” in California would subject the data to CCPA. What if that same “domiciled” person spends long periods of time in another state—is all their data subject to CCPA, or does it only apply to data generated when the consumer was physically present in the state?

Conclusion

Hitachi lauds the Board’s efforts and looks forward to continuing to work with the State of California as CCPA continues to evolve.

Sincerely,



Hicham Abdessamad
CEO & Chairman
Hitachi America, Ltd.

From: **Andrew Kingman** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment - State Privacy & Security Coalition
Date: 23.08.2022 16:40:33 (+02:00)
Attachments: SPSC - CPRA Draft Regulation Comments - 08.23.22.pdf (12 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,

On behalf of the State Privacy & Security Coalition, please find attached comments regarding the draft CCPA regulations. We would be happy to answer any questions you may have.

Respectfully submitted,
Andrew Kingman

Andrew Kingman

President



www.marinerstrategies.com



STATE PRIVACY & SECURITY COALITION

August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: State Privacy & Security Coalition Comments on CCPA Regulations

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

The State Privacy & Security Coalition, a coalition of over 30 companies and trade associations in the retail, technology, automobile, telecommunications, and payment card sectors, respectfully submits the following comments regarding the proposed California Consumer Privacy Act (CCPA) regulations.

Our coalition works in all 50 states on data privacy and cybersecurity legislation and regulations. We evaluate proposals to ensure that they appropriately balance increased control and transparency for consumers, operational workability for businesses, and cybersecurity protections for all stakeholders.

Unfortunately, the California Privacy Protection Agency (CPPA, or the Agency) has proposed regulations that clearly exceed its statutory authority granted by its enabling text. In so doing, the Agency's initial draft does not meaningfully benefit consumers, nor does it increase the operational workability for businesses. These comments detail those provisions; we request that they be struck from the final regulations due to this violation of statutory authority.

Standard of Review

A regulation is invalid if: 1) it is not "consistent" with the statute; 2) it is "in conflict" with the statute; 3) it is not "reasonably necessary to effectuate the purpose of the statute"; or 4) it is "not within the scope of authority conferred" by the statute.¹

Opt-Out Preference Signal (OPS)

The Agency has clearly exceeded its authority by using the proposed regulations to state that the OPS is mandatory for businesses to recognize. While this may be the Agency's preference, the edict is in conflict with the plain text of the statute.

The California Privacy Rights Act (CPRA) modifies California Civil Code 1798.135 by renaming the section "Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information." Within this section, the statute provides that a business may choose one of two methods to allow consumers to limit the sale of personal information, the sharing of personal information, and to limit the use of sensitive personal information:

¹ Cal. Gov. Code §§ 11342.1; 11342.2.

STATE PRIVACY & SECURITY COALITION

Method 1 (using clear and conspicuous links):

- a. Provide a clear and conspicuous link on each website page that collects personal information titled “Do Not Sell or Share My Personal Information;” and
- b. Provide a clear and conspicuous link on each website page that collects personal information, titled “Limit the Use of My Sensitive Personal Information;” or
- c. At the business’s discretion, a single link that accomplishes both tasks, “if such a link easily allows” a consumer to both opt-out of the sale/share of personal information and limit the use of sensitive personal information; or

Method 2:

- a. Recognizing an OPS.

Critically, subparagraph (b) of §1798.135 states that: “A business *shall not be required to comply with subdivision (a)* if the business allows consumers to opt-out of the sale or sharing of the personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism...” (emphasis added).

Put quite simply, the CPRA sets forth two ways that a business may allow a consumer to opt-out/limit the use of their personal information and sensitive personal information: the first, by offering either two separate links or one combined link (subdivision (a)), or the second by recognizing an OPS (subdivision (b)).

However, the Agency seeks to impose a requirement that recognition of an OPS be mandatory for businesses – again, clearly in conflict with the plain text of the statute. In §7026(e), the Agency proposes an unusual regulation, stating in part that “Civil Code Section 1798.135...does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals...” The Agency contorts the plain text of the statute into a reading that a business *must* recognize an OPS, but *may* choose to post the links.

The Agency states in its Initial Statement of Reasons that its proposed regulation making the OPS mandatory “is...necessary to address a common misinterpretation of Civil Code section 1798.135, subdivisions (b)(3) and (e), that complying with an opt-out preference signal is optional for the business. Not so.”

There is no basis in the statute for this interpretation; in fact, other parts of the statute directly contradict the Agency’s unfounded interpretation. Notably, Civ. Code §135(b)(3) states *explicitly*:

“A business that complies with subdivision (a) of this Section [posting links] *is not required to comply with subdivision (b)* [using OPS]. For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).”

STATE PRIVACY & SECURITY COALITION

The plain text of the statute undermines the Agency’s assertion of its policy preferences. The OPS is quite clearly a provision designed to be optional, not mandatory. Section 185(a)(20) gives the CCPA a charge that includes “[i]ssuing regulations to govern how a business *that has elected to comply with subdivision (b)* responds to the opt-out preference signal....” (emphasis added). Again, this is dispositive evidence of the CPRA’s intent – a clear statement that a business can choose whether to comply with subdivision (a) (posting links) or with subdivision (b).

California courts have rejected regulatory interpretations that contradict the plain text of the governing statute when the agency’s interpretation is “at war with the straightforward textual conclusion.”² We submit that this “straightforward textual conclusion” is in fact what the Agency mischaracterizes as business’s “common misinterpretation.” The Agency’s policy position, manifested in these regulations, is not simply inconsistent with the statute – it is in direct conflict. The regulations stating the OPS is mandatory must, by law, be removed from the Agency’s final version.

Additionally, these regulations fail to set forth common, clear technical guidance or disclosure requirements for opt-out signal developers. The current regulations ignore important requirements set forth in Section 1798.185(a)(19) of the CPRA, such as ensuring the opt-out signal clearly represents a consumer’s intent, is free of defaults presupposing such intent, and does not conflict with other commonly used privacy settings and tools. These requirements cannot be satisfied unless an opt-out signal is capable of identifying California residents and presenting the user with specific information about any technical limitations of the signal and the applicable Do Not Sell or Do Not Share My Personal Information under the CPRA.

Put another way, responsibility should lie with the OPS developers to ensure that its users understand how the signal works, as well as its limitations. Otherwise, the lack of guidance puts an unreasonable burden on businesses to sort through various signals with differing specifications, which will considerably impede the adoption and workability of the OPS.

Collection of Personal Information

The OPS is not the only area where the Agency’s proposed regulations exceed the scope of the statute. The CCPA as amended by the CPRA requires that:

[C]ollection, use, retention, and sharing of a consumer’s personal information shall be *reasonably necessary and proportionate* to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is *compatible with the context in which the personal information was collected*, and not further processed in a manner that is incompatible with those purposes. (emphasis added).³

² *In re McGhee*, 34 Cal.App.5th at 905

³ Cal. Civ. Code §1798.100(c)

STATE PRIVACY & SECURITY COALITION

This paragraph sets forth two standards for the processing of a consumer's personal information. Processing is permissible when:

1. The collection, use, retention, and sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purposes for which the information was collected or processed;
2. The collection, use, retention, and sharing of a consumer's personal information shall be:
 - a. reasonably necessary and proportionate to achieve...another disclosed purpose that is compatible with the context in which the personal information was collected, and
 - b. not further processed in a manner incompatible with those purposes.

In other words, the necessary tests for processing information are either the reasonably necessary and proportionate standard, or the compatible purpose standard. However, the proposed regulations would yet again depart from the statutory mandate by including additional and contradictory requirements that could fundamentally restructure the CCPA from a largely opt-out framework to a much more burdensome opt-in framework even for purposes compatible with the context in which the personal information was collected. This contradicts the intent of the statute.⁴

Specifically, §7002(a) of the proposed regulations could dramatically alter this provision by impermissibly expanding its scope. The section states that “to be reasonably necessary and proportionate, the business’s [processing] must be consistent with what an average consumer would expect when the personal information was collected.” The proposed regulation departs from the language of CPRA, which permits using covered data “for another disclosed purpose that is compatible with the context in which the personal information was collected.”

This is problematic in several ways. First, the regulations do not specify what the “average consumer” standard means. Second, this new standard shifts the focus from the nexus between the compatibility of a disclosed purpose for processing information to the Agency’s interpretation of what the average consumer would expect of the use, creating a clear inconsistency with the existing text, and doing so in a way that would enlarge its scope. Agencies do not have discretion to promulgate regulations that are inconsistent with the governing statute, or that alter or amend the statute or enlarge its scope.⁵

⁴ “...by moving to an opt-in regime where consumers have to assess risk, opt-in, and consent to the use of their information, not only are they not going to be able to understand and consent for immediate benefits...they’re also going to experience opt-in fatigue when they’re just going to opt-in to whatever the service is, like free coffee, in order to get that benefit today at the risk of anything that happens tomorrow.” – Ashkan Soltani, March 5, 2019, California State Senate Judiciary Committee hearing, available at <https://www.senate.ca.gov/media/senate-judiciary-committee-20190305/video>

⁵ See *Henning v. Div. of Occupational Saf & Health*, 219 Cal.App.3d 747, 760 (nullifying a regulation because “[a]dministrative regulations that alter or amend the statute or enlarge or impair its scope are void”)

STATE PRIVACY & SECURITY COALITION

The Agency further enlarges the scope of this provision by adding an opt-in consent requirement for any processing that “is *unrelated* or incompatible with the purpose(s) for which the personal [was] information collected or processed.”[sic].⁶ Here again, the Agency creates a standard not found in the statute, which only speaks to the compatibility standard.⁷ These standards are distinct. There are clear examples where important processing of personal information may be “unrelated” but not “incompatible.” One can easily imagine a business collecting personal information for security purposes, and where this is disclosed to the consumer – but where it is unrelated to the purpose for which it was collected. The Agency lacks authority to create an “unrelated” standard where the statute clearly creates a “compatibility” standard – these standards are distinct.

This section of the regulations creates ambiguity as to which purposes will be considered compatible, and which processing will be considered necessary and proportionate. The Agency’s lack of examples for what would be considered either necessary and proportionate, or compatible with consumer expectations, suggests a policy preference to move the statute to a more intensely opt-in framework that is unsupported by either the history or the text of the statute.

In straying from the language and clear intent of the CCPA as amended by the CPRA, the Agency also exceeds its statutory limits with these proposed rules because the CPRA *does not grant rulemaking authority on this point*. In its Initial Statement of Reasons, the Agency cites Cal. Civ. Code §1798.185(a)(10), stating that § 7002 “reflects the mandate set forth in...1798.185, subdivision (a)(10), that the purposes for which businesses may use consumers’ personal information should be consistent with consumers’ expectations.”

However, there is no text in this section that provides the Agency *any authority* to regulate the *methods of collection*; it gives the Agency authority to delineate specific business purposes in addition to those set forth in 1798.140(e). §1798.185(a)(10) gives the Agency authority *only* for “further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers’ personal information with consumers’ expectations, and further defining the business purposes for which service providers and contractors may combine consumers’ personal information obtained from different sources...”

Because the Agency is attempting to issue regulations that it lacks the statutory authority to issue, and because such regulations impermissibly enlarge the scope of the statute from restrictions that focus on what is reasonably necessary and proportionate, or compatible with the disclosed purposes to a new opt-in requirement with an undefined “average consumer” standard, SPSC requests that this provision be removed from the final regulations.

⁶ Proposed Regulations, 7002(a) (emphasis added)

⁷ See Cal. Civ. Code §1798.100(a)(1)-(2), (c).

STATE PRIVACY & SECURITY COALITION

A better, more helpful approach would be to look to Europe’s General Data Protection Regulation (GDPR), where Recital 50 sets forth an interpretation of compatibility that many companies already employ in Europe.⁸ The guidance promulgated by the European Commission sets forth several considerations that help entities determine whether their uses are compatible with the purposes for collection, including:

- The link between the original purpose and the new purpose;
- The context within which the data was collected;
- The type and nature of the data;
- The possible consequences of the intended further processing; and
- The existence of appropriate safeguards (e.g., encryption or pseudonymization).

The Agency’s lack of interest in creating interoperability between California’s privacy regime and other regimes continues to be a source of frustration for businesses who are attempting to comply with this global patchwork. Further, the Agency’s lack of positive examples that could illustrate any reasonable path to compliance is also frustrating to companies that are diligently working to ensure their programs are consistent with the CPRA. As the Agency works to adjust its regulations to be consistent with its authority under the statute, it should strive for rules that are interoperable and include positive examples.

The Regulations Impermissibly Alter the Scope of the Business and Service Provider Duties and Responsibilities

The CPPA further exceeds the limits of the statute by imposing new performance, contractual, and legal requirements on entities who are entitled by the CCPA’s statutory text to determine whether they are functioning as businesses, service providers, contractors, or third parties. The regulations also impermissibly attempt to add in a duty of diligence for businesses that is simply not contemplated in the text of the CPRA.

a. The Draft Regulations Defy the Statutory Definition of “Service Provider” and Confuse the Classification of Entities

The CCPA sets forth very clearly the central component to being a service provider: the existence of a contract with a business that limits the service provider’s use of information to only that which is set forth in the contract.⁹ A third party is defined in the negative as an entity that is neither a consumer-facing business, a service provider, nor a contractor.¹⁰

But the regulations impose requirements on service providers by requiring them to be service providers *even when they are not providing services to a business*. §7050(a) states that any entity that provides services to a non-business “and that would otherwise meet the

⁸ <https://www.privacy-regulation.eu/en/recital-50-GDPR.htm>

⁹ “Service provider” means a person that processes personal information on behalf of a business...pursuant to a written contract...” Cal. Civ. Code 1798.140(ag)(1)

¹⁰ Cal. Civ. Doe 1798.140(ai)

STATE PRIVACY & SECURITY COALITION

requirements and obligations of a ‘service provider’ or ‘contractor’ under the CCPA and these regulations, *shall be deemed a service provider or contractor* with regard to that person or organization for purposes of the CCPA and these regulations.”

This introduces numerous ambiguities that these regulations leave unanswered, including: do entities providing services to a non-profit but that do not have a contract now need to negotiate a contract? If there is an existing contract, does it now need to be modified to reflect the requirements of a service provider contract? Can a non-business that transfers personal information to another entity that assumed it was a third-party due to the lack of a contract bring an action against that entity for violating service provider use requirements?

With this provision, the Agency has fundamentally changed a key component of the CCPA – the classification of entities. This classification is absolutely critical, because all of the obligations, relationships, and liabilities flow from an entity’s status. The service provider definition is crystal clear that a service provider is an entity that processes personal information *on behalf of a business*. The regulations clearly exceed the scope of this definition and should be removed or re-written as SPSC proposes below.

Additionally, the Agency seeks to promulgate regulations that would further put service providers in an untenable legal purgatory. §7051(c) states that “a person who does not have a contract that complies with subsection (a) is not a ‘service provider’ or a ‘contractor’ under the CCPA.” The example provided states that “a business’s disclosure of personal information to a person who does not have a contract that complies with these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.”

For entities that are providing services to entities that are not businesses as defined by the CCPA, this puts them in an untenable bind. By transferring personal information to this non-business, are they deemed to be a service provider, as subsection (a) states? Or are they a business that is “selling” information to another entity, as subsection (c) states. This ambiguity is confusing, unnecessary, and punitive in a way that is clearly inconsistent with the statutory text. Effectively, the regulations ensure that an entity providing services to a non-business can never be sure of its standing until there is a regulatory determination of which type of entity it is under California law. Surely this lack of clarity is not a positive policy direction for California or the CCPA.

Again, the stated authority that the Agency cites to promulgate these rules finds no basis in the actual text. The Agency, in its initial statement of reasons, states that it draws authority from Cal. Civ. Code 1798.185(a)(10) and (11) – and yet these require only regulations *identifying the business purposes and circumstances under which a service provider or contractor may use and/or combine consumers’ personal information*. There is *no* authority to fundamentally reconsider the delineations set forth in the CCPA about the nature of the classifications themselves. This alters and amends key definitions, which is not permitted by California law. An

STATE PRIVACY & SECURITY COALITION

agency “cannot enlarge the scope of the statute by simply promulgating a rule purporting to define [a term] differently” than it is defined in the statute.¹¹

SPSC recognizes that 7050(a) serves a productive purpose outlined in the Initial Statement of Reasons – namely, the avoidance of service providers being responsible for fulfilling consumer rights requests that are tendered to, for example, a non-profit, or a for-profit entity that does not meet the definition of a “business.”

However, that benefit alone can be solved with simple clarifying language that we would propose in place of both §7050(a) and §7051(c): “A service provider or contractor is not responsible for any obligations under this Act when it is providing services to an entity that does not meet the definition of a business, as defined in §1798.140(d).” This is a much clearer way to state the helpful purpose of these regulations without the unintended consequences that flow from the inclusion of both of the above-referenced sections.

b. The Regulations Impose Requirements on Service Providers that Do Not Have a Basis in the Statute.

The regulations also attempt to impose a duty of diligence on businesses with regard to service provider and contractor compliance with these laws. This duty of diligence is not contemplated in either the original CCPA or the CPRA amendments.

A company must be able to rely on the representations made in a contract with a service provider or contractor, and this is reflected in § 1798.145 (i). However, §7053(e) of the proposed regulations undermines these protections. The illustrative example, that a business that “*never exercises its rights to audit or test the service provider or contractor’s systems might not be able to rely on this defense...*” may be read as a de-facto monitoring obligation, above and beyond the requirements of CPRA. While many companies have in place auditing programs of their service providers/contractors, the frequency of such audits are generally correlated with the level of risk that the personal information being processed represents, anywhere from 1 to 3 years, depending on the nature of the contract and the services. The proposed regulations could therefore require unduly onerous ongoing monitoring obligations of service providers or contractors which erodes the principles of service provider/contractor responsibility in the CPRA.

c. The Regulations Attempt to Prohibit Statutorily Permissible Advertising Activity

The illustrative example in Section 7050(c)(1) of the draft rules goes beyond the textual bounds of the statute and raises new questions and uncertainty for businesses beyond those called out in the example.

¹¹ See *People ex rel. Dep’t of Alcoholic Beverage Control v. Miller Brewing Co.*, 104 Cal. App. 4th 1189, 1198-99 (2022).

STATE PRIVACY & SECURITY COALITION

The illustrative example purports to prohibit a form of advertising based on email addresses, and it is unclear what the basis is for doing so. The CPRA's delineation of "advertising and marketing services" as a permissible business purpose prohibits the combination of personal information for a business's opted-out consumers with a service provider's information obtained on its own or from other entities. However, the illustrative example appears to suggest that *any* combination of information by a service provider is impermissible, not just the combination of personal information of opted-out consumers.

The implications of this example would be significant; this would create uncertainty regarding CPRA's treatment of relationships between businesses and service providers with respect to advertising as well as more broadly with respect to future contracts between businesses and service providers. SPSC proposes clarifying the example as follows:

"The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third-party businesses' websites, applications, or services."

Right to Correct

While the statute gives the Agency authority to promulgate rules about the right to correct, the Agency has drafted these rules to contradict core features of the statutory framework.

First, the draft regulation includes an obligation to provide the consumer with the name of the source from which the business received information the consumer claims is inaccurate. This is unworkable and does not properly take into account the "burden on the business" that the Agency is required to consider pursuant to 1798.185(a)(7). Additionally it raises commercial confidentiality issues, as well as security issues that the Agency is required to consider.

Conceptually, this requirement is in tension with the CCPA as amended by the CPRA, which does not require this type of disclosure even under the broad right to know and access rights. The statute consistently calls for companies to disclose categories of sources, but not specific sources. In stark contrast, under this proposed right to correct, companies would have to divulge specific sources.

Second, the provisions requiring a business to "disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct" is overly broad. At a minimum, this should only apply to the specific pieces of PI relevant to the request to correct and should be subject to the same protections that the right to know responses are subject to (e.g., prohibition on disclosing sensitive PI like biometrics and SSN). Otherwise, this overly broad access rule would serve as a

STATE PRIVACY & SECURITY COALITION

loophole for the reasonable security parameters in place to protect against the access right being used to harm rather than help consumers—which is foundational to the CCPA framework. Lastly, it is likely that many requests to correct personal information do not require this type of burdensome disclosure. The Agency is also required to promulgate rules pertaining to corrections with “the goal of minimizing the administrative burden” on consumers.”¹²

12-Month Look-Back Period

The regulations further exceed the scope of the CPRA by requiring businesses to provide personal information beyond the 12-month period contemplated by the CCPA as amended by the CPRA. There, §1798.30 explicitly sets forth the process for granting a consumer request:

“the disclosure of the required information shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request, provided that, upon the adoption of a regulation...***a consumer may request*** that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort.” (emphasis added).

The referenced regulation (§1798.185(9)) states that the CPPA shall establish “the standard to govern a business’s determination...that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.”

However, the draft regulation neither recognizes the centrality of the consumer’s role in requesting personal information beyond the 12-month period, nor does it attempt to elucidate a standard to govern a business’s determination of impossibility/disproportionate effort.

Instead, the draft regulation eviscerates the distinction between information provided within and outside the 12-month period, stating that a business is responsible for providing all personal information in response to a request to know, “including beyond the 12-month period preceding the business’s receipt of the request, unless doing so proves impossible or would involve disproportionate effort.”

Even the Agency’s own summary of its regulations concede that it ignores the text of the statute, stating that the regulations in part “[e]stablish procedures to extend the 12-month period of disclosure of information” in response to a consumer request.¹³

In the body of the Initial Statement of Reasons, the Agency claims that the regulations have “been revised to align the regulation with the revised language of the statute.” As

¹² Cal. Civ. Code 1798.185(a)(7)

¹³ Initial Statement of Reasons, p.2 par. 2

STATE PRIVACY & SECURITY COALITION

demonstrated above, however, *nowhere does the regulation permit the Agency to extend this time period* by default and without a consumer request. It *only* provides the Agency with authority to clarify how a business may determine that providing the personal information beyond the 12-month period is impossible or involves disproportionate effort.

There are significant operational implications to this overreach. In the effort to meet the January 1, 2023 implementation deadline, businesses and service providers are designing their data storage architecture to be able to retain, store, and retrieve consumer personal information in ways that are sufficient for statutory compliance. By changing the default time period for retrieving personal information from “12 months” to “indefinitely,” the Agency is not only significantly altering the statute’s expressed policy preference, but is also making it operationally difficult to build compliant systems.

Again, this draft regulation is a clear case of the Agency using this process as a way to expand the scope of the CPRA – something which is not permitted by California law.¹⁴ Policy considerations do not trump the plain text of the governing statute.¹⁵

One-Year Enforcement

The intent of the CPRA’s language regarding enforcement is that it should begin no earlier than one year following adoption of the final regulations. The CPRA states that final regulations shall be adopted by July 1, 2022. Clearly, the regulations will be adopted substantially later than this – sometime in the fourth quarter of 2022.

Accordingly, SPSC believes that in order to appropriately honor the CPRA’s intention regarding enforcement, that the Agency refrain from any enforcement action for a period of one year following the final adoption of these regulations.

These regulations contain substantial modifications and additions to the CPRA, and businesses need time to rework many of the systems they were in process of implementing in order to be in a compliance posture. They should not be held to an artificial timeline for implementing the rules that themselves took longer than anticipated to finalize.

Audit/Enforcement Powers

While SPSC does not argue that the CPRA provides authority for the CPPA to establish processes for the Agency to audit companies, we take strong issue with the process set forth in these regulations. It would be difficult to imagine a process designed to be more heavily weighted in the government’s favor and with less due process for California businesses than the one set forth in §7304. In sharp contrast to the process set forth in §7302 closely tied to a recognizable

¹⁴ *In re McGhee*, 34 Cal.App.5th at 905.

¹⁵ *Id.*

STATE PRIVACY & SECURITY COALITION

legal standard, the process described in §7304 lacks any limits on the Agency’s power or the delineation of standards to which businesses and service providers can expect to be held.

If this section is adopted as is, the CPPA will have the right to a) audit companies without notice; b) make a determination without any opportunity for rebuttal that a subject’s processing of personal information presents “significant risk to consumer privacy,” and states that the consequence for any company’s “failure to cooperate” during an unannounced, unjustified audit is a “subpoena...warrant, or otherwise exercising [the CPPA’s] powers.”

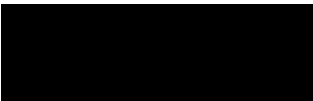
Surely, more narrowly tailored audit provisions are possible while still retaining strong enforcement powers. SPSC proposes removing the ability of the CPPA to: 1) conduct unannounced audits; 2) make a “significant risk” determination with no documentation, process, or justification; 3) provide an ability for a company to respond to an audit request in a manner that, if legitimately reasonable, would obviate the need for such request.

SPSC also proposes that the scope of any audit request should be approved by CPPA members prior to being issued, and that a business’s election to participate in an audit be considered a mitigating factor in any subsequent enforcement decision.

Conclusion

A regulation is invalid if it is not “consistent” with the statute, if it is “in conflict” with the statute, if it is not “reasonably necessary to effectuate the purpose of the statute”, or if it is “not within the scope of authority conferred” by the statute. In attempting to promulgate these draft regulations, the Agency has clearly exceeded its authority in several sections. The State Privacy & Security Coalition respectfully requests that the above-referenced draft regulations be removed from the final version.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

From: **Gabriel Acosta** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 16:54:14 (+02:00)
Attachments: MBA CAMBA CPRA Letter.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Members of the California Privacy Protection Agency,

Please see the attached comments by the California Mortgage Bankers Association and the Mortgage Bankers Association on the proposed implementation of the California Privacy Rights Act.

Respectfully,
Gabriel Acosta
Regulatory Specialist

[REDACTED]

This email is intended for the recipient specified in the message only. If you received this message by mistake, please reply to this message to inform the sender of the mistake, so that the sender can ensure such a mistake does not occur in the future. If received in error, you should promptly delete this email from your system. Do not share this message with any third party without the written consent of the sender.



August 23, 2022
Brian Soublet
California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: Proposed Rules to Implement the California Privacy Rights Act

Dear Mr. Soublet,

The California Mortgage Bankers Association (CAMBA)¹ Mortgage Bankers Association (MBA)² and would like to thank the California Privacy Protection Agency (CPPA) for the opportunity to comment on the Agency's proposed regulations (Proposed Regulations), under the California Privacy Rights Act (CPRA). While most of the data our members use is exempted from the act under the Gramm-Leach-Bliley Act (GLBA) exemption, we offer the following feedback to improve the regulation's ability to protect consumers and be implemented consistently and successfully.

Maintaining up-to-date data security practices remains a top priority for the real estate finance industry. Since GLBA passed in 1999, the financial services sector has operated under a comprehensive privacy and data security regime. Protecting personal information is both an existing regulatory requirement and allows MBA members to maintain the trust of their

¹ The California MBA, representing hundreds of companies and tens of thousands of California employees, is the leading advocate for the industry in the largest mortgage/real estate market in the nation. The California MBA represents residential and commercial/multi-family mortgage bankers, as well as their essential vendor partners. The California MBA encourages and promotes sound business practices and honesty in marketing, origination, lending, and servicing of mortgage loans through our educational and networking opportunities.

² The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 330,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 1,700 companies includes all elements of real estate finance: independent mortgage banks, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, credit unions, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

customers. Each year, financial firms expend significant amounts of time and resources to safeguard consumer data, protect data from malicious actors, and defend against adversaries that target financial institutions. Financial institutions develop data security plans, train their front-line employees in best practices, and hire experts to implement protective measures for the mortgage industry.

MBA members already devote a great deal of attention to compliance and data security regulations. These regulations, requirements, and guidelines are enforced by dozens of regulatory bodies exercising overlapping jurisdiction, including but not limited to the Commodity Futures Trading Commission, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Federal Reserve System, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Financial Industry Regulatory Authority, and the Consumer Protection Financial Bureau. Many other data security regulations have been issued in accordance with the GLBA, a law specifically tailored to consider the needs of financial institutions and their customers. GLBA's implementing regulations set uniform requirements with respect to the development and maintenance of comprehensive data security programs. These comprehensive requirements govern all areas of data protection and consumer privacy.

California is the state with the biggest market for mortgage products. This market share leads many states' policy makers to adopt California's standards in those other states. In attempting to emulate California, however, other states may establish a divergent approach. It is important to note that each MBA member company maintains a single technology infrastructure, and not one for each set of state and federal requirements. For these reasons, MBA believes a longer deliberative approach is appropriate here. Many of the agencies listed above are engaged in rulemaking on data security. The CFPB just announced new policies on data privacy, and the FTC is actively engaged in rulemaking on this issue.³ Additionally, Congress is currently debating the American Data Privacy and Protection Act (ADPPA), which would overhaul the current data security regime. As currently drafted, this legislation would strip significantly reduce the rulemaking authority of the CPPA. Given the tumultuous time in both the regulatory space and the mortgage market, we urge caution in developing regulations that may need to be amended quickly or overhauled entirely.

MBA members support strong, uniform data security practices. We ask that the Proposed Regulations create clear and actionable guidelines that will help control compliance costs and protect consumer data. MBA and its member companies would like to encourage the CPPA to consider the following changes to the proposed rules:

- Provide definitive guidance regarding practices related to dark patterns,
- Clarify what must be considered when determining disproportionate effort and,
- Include additional clarity for the "average consumer" standard.

³ Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2022-04, "Insufficient data protection or security for sensitive consumer information" (Aug. 11, 2022), available at <https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/>; Federal Trade Commission, Commercial Surveillance and Data Security Rulemaking (Aug. 11, 2022), available at <https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking>.

Dark Patterns

MBA has some concern related to the lack of specific guidance for dark patterns and how business entities should avoid them when interacting with consumers. Dark patterns are defined in Cal. Civ. Code § 1798.140(l) as, “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation.” Under the definition of consent⁴, use of a dark pattern to obtain consent voids the consent. Section 7004 of the Proposed Regulations specifies that for a business to provide a consumer choice that does not present a dark pattern, the business must present a choice that is easy to understand, offer symmetrical choices, avoid confusing the consumer or using manipulative language, and be easy to execute.

In the Proposed Regulations there is no consideration for the material nature of the item consented to or business intent before voiding consumer consent. Currently, a dark pattern presented to a consumer over any innocuous item can destroy consent for every other piece of information used or collected. Additionally, Section 7004(c) specifically precludes any consideration of business intent. Therefore, a well-meaning business, which inadvertently structures its interface in a manner that could be construed to be a dark pattern to obtain a piece of data for a limited purpose could void consumer consent for the collection of important information related to their financial transaction. This could potentially imperil a consumer home loan if a lender was unable to achieve proper consent due to an unintended mistake that could be alleged to be use of dark patterns.

In addition, this section does not prohibit many specific practices, and instead uses subjective measures with a high level of generality to prohibit practices. The Proposed Regulations refer to standards such as an “easy to understand” interface or language “confusing to the consumer”, which are subjective measures that will change over time. These fact-specific standards also create significant legal uncertainty as they are difficult to define concretely and ripe for subjective application. The regulations should provide more clarity about the specific practices that are prohibited under this section to provide clarity and help prevent inadvertent violations of the CPRA statute and regulations.

Disproportionate Effort

The Proposed Regulations give businesses a defense when complying with consumer requests in Section 7001(h). A business may deny certain requests if complying requires disproportionate effort. This is a measurement of whether the resources and time a business uses to respond to a consumer request significantly outweighs the benefit provided to the consumer by responding

⁴ “Consent” means any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent. Cal. Civ. Code § 1798.140(h).

to that request. Businesses must show that the time and resources needed to execute a request are significantly higher than the material impact on the consumer.

However, this defense relies on subjective or hard to quantify measures that must be disclosed in a factually detailed enough explanation to give consumers a meaningful understanding of the denial. For a business to show that processing a request would require disproportionate effort, they would need to retain many documents on measures that are difficult to quantify. For example, how would a company quantify the “time and or resources” required to complete a request, especially in cases where it is not clear from an initial review how to comply with a request. It is not clear how a business would measure the benefit or material impact to the customer, especially when the reason for the request is not known. Making a business determine the material impact to consumers is a vague and subjective task, requiring the business to read the mind of the consumer. In addition, a factual and detailed denial would have to include an explanation of a financial institution’s technical processing platform. Giving this level of detailed information will both confuse consumers and could force financial institutions to disclose trade secrets.

This balancing test is further complicated by the example the CPPA uses in the Proposed Regulations. The example given of a request that would require disproportionate effort is one in which denying the request “would not impact the consumer in any material manner.” This potentially creates confusion and does not show the tradeoffs businesses are supposed to consider when making this decision. If this is the median case, then this provision is not a balancing test and would require businesses to process a request unless there is no material impact to the consumer. The CPPA should consider providing additional clarity in how to effectively balance these conditions to make the proper compliance decisions.

This defense is intended to allow businesses to prioritize their resources towards answering requests from consumers in need. As written, much time and many resources will need to be spent answering cumbersome or unnecessary requests. We ask for more particularity so our members can prioritize the consumers this Proposed Regulation is intended to help.

“Average Consumer” Standard

The Proposed Regulations tailor several requirements according to an “average consumer” standard and what that potential individual would expect. Although this is a commonly used legal standard, there needs to be additional clarity in the proposed rules because of the quickly evolving nature of technology. As new technology emerges, the average consumer’s expectation will change over time. However, it is hard to know what the “average consumer” can expect given wide variance in technological capacities and literacy across the general population.

There are other problems with creating a regime based on consumer’s expectations. A first party is defined as, “the consumer-facing business with which the consumer intends and expects to interact.” This definition is meant to distinguish first parties from third parties. Defining first parties according to consumer expectation raises problems, especially in the mortgage context. For instance, it is not clear if the average consumer knows that servicers and not the originating lenders are responsible for facilitating loan default. The CPRA places different duties on parties

depending on these categories. Creating a regulatory regime based on shifting or factually incorrect consumer beliefs only creates confusion and regulatory risk for businesses.

Once again, thank you for providing us with the opportunity to comment on the Proposed Regulations. Our association welcomes the opportunity to engage with you further to develop California's data privacy regulations. If you have any questions, please contact Kobie Pruitt [REDACTED] or [REDACTED]).

Respectfully,



Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association



Pete Mills
Senior Vice President
Residential Policy and Member Engagement
Mortgage Bankers Association

From: **Matthew Powers** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **John Shirikian** [REDACTED]; **Matt Akin** [REDACTED];
John W. Mangan [REDACTED]; **Kristin Abbott** [REDACTED]
Subject: CPPA Public Comment: ACLI and ACLHIC
Date: 23.08.2022 17:49:11 (+02:00)
Attachments: ACLHIC ACLI CPRA Reg Comment Letter 8.23.22 (Final).pdf (6 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To Whom It May Concern:

Please see attached comments from the American Council of Life Insurers (ACLI) and the Association of California Life and Health Insurance Companies (ACLHIC) on behalf of the life insurance industry in California.

Regards,
Matthew Powers

--

ACLHIC

P: [REDACTED]

www.aclhic.com



August 23, 2022

Mr. Brian Soublet, Director
 California Privacy Protection Agency
 2101 Arena Blvd., Sacramento, CA 95834
 Email: regulations@coppa.ca.gov

Re: *Comments on Proposed Regulations to Implement the Consumer Privacy Rights Act of 2020 (CPRA)*

Dear Director Soublet:

The American Council of Life Insurers (ACLI) and the Association of California Life and Health Insurance Companies (ACLHIC) respectfully submit the following comments on behalf of our members in response to your Notice of Proposed Rulemaking released July 8, 2022. We appreciate your efforts to implement the CPRA, and believe there are several areas where California's consumers and businesses would benefit from additional changes and clarifications to the proposed language.

Of note, life insurers have historically served as conscientious stewards of our customers' highly sensitive personal information. We abide by and support strong consumer privacy. We have managed consumers' confidential medical and financial information appropriately for decades, and in the instance of several of our member companies, a couple of centuries. We look forward to working with you and lending our industry's historical expertise to this weighty issue.

Please find below our comments and suggested revisions by section:

General Comments:

The requirements that these proposed regulations will place on insurers will require significant resources for regulatory compliance. Given the delay in providing draft regulations and the hyper-technical nature of the regulations, we respectfully request a delayed compliance date of at least 1 year from the date the regulations are adopted and explicit prospective, not retroactive, applicability.

We also encourage CPPA to use existing well tested formats for compliance that would make notices more understandable. We think that there is an apparent effort to enable a consumer-friendly presentation of privacy options, but at the same time there are requirements for a host of new popups, links, and disclosures for website and in-person application. These new requirements are inherently at odds with "consumer-friendly" presentation of privacy options. Using existing, well tested formats for compliance will bring these requirement's more into line with the consumer-friendly approach the regulations seek.

Article 1: General Provisions

7001. Definitions

(r): We appreciate the explicit reference in the Agency's Initial Statement of Reasons to global privacy controls as an example of an opt-out preference signal. However, we think this section, or 7025(b),



requires more clarification and confirmation that a “do not track” signal is not sufficient to be considered a request to opt-out of data selling and sharing.

7002 Restrictions on the Collection and Use of Personal Information

(a) We believe that the language referencing what an average consumer would reasonably expect creates an unrealistic compliance standard, and recommend subsection (a) be replaced with the following language as it provides a clearer expectation: "A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) disclosed in the notice at collection."

Article 2: Required Disclosures to Consumers

7011 Privacy Policy

(e)(1)(H), (I), and (J): For the purposes of the privacy policy we believe that these three paragraphs which reference disclosure of personal information are overly broad, and these types of disclosures should be limited to sale and share, as indicated in (D), (E), and (F). We believe this is more in keeping with the underlying purpose of the CCPA and CPRA, and provides consumer with more specific and useful information.

(e)(3)(F) and (G): We believe businesses that do not sell or share personal information should be clearly exempted from these requirements to disclose in their privacy policy how the business would process opt-out preference signals. As drafted this requirement would create significant confusion for consumers about whether their Personal Information is being sold or shared.

7012 Notice at Collection of Personal Information

In instances where the only in-scope personal information that a business is collecting is for the purpose of cross context behavioral advertising, we believe that companies should not be required to post a notice at collection since this is already required in the privacy notice as well as the opt-out notice which provide the same information. Adding yet another notice in this case simply adds confusion for the consumer and is an unnecessary burden on companies.

(e)(6) We request deletion of this provision as it does not benefit, and may create confusion for, consumers. It is not clear what it means for a third party to control the collection of personal information. Would this include any cookies and/or pixels companies use on their websites? As third parties are likely to change over time we believe that the requirement to disclose all third parties that a business uses would be too administratively burdensome, would open the potential for bad actors to target certain products and services and could be anti-competitive. We are also unclear what type and level of detail "information about the third parties' business practices" is intended to mean. Lastly, as businesses are required to provide this information in response to consumer requests, there is no actual benefit to the consumer for this information to be shared publicly.

(g)(2) We believe that the reference to information about the “business practices” of the third-party lacks clarity. Specifically what type and level of detail the third party is required to disclose.



(g)(4)(C) We appreciate the effort to provide illustrative examples for compliance purposes, however we find this example confusing. What is the relationship between the three companies? Specifically, how does business M relate to the other two businesses?

7013 Notice of Right to Opt-Out of Sale/Sharing and the Do Not Sell or Share My Personal Information Link

For businesses that may find compliance with icon size requirements in 7015 challenging, but only share data, it would be confusing to consumers if these businesses were required to use the language that indicates to consumers that they are engaged in the sale of data. We request that 7013 allow businesses to post a link stating only, “Do Not Share My Personal Information” if the business is not engaged in the sale of data.

7015 Alternative Opt-Out Link

(b) Icon sizes across a website might not be consistent, so we respectfully ask for clarification for what a business should do if there is variance in icon size. What size should the alternate opt-out link approximate? We believe it would make sense for the icon to be approximately the same size as the link or links it is next to and not to other icons on other parts of the business’s website.

Article 3: Business Practices for Handling Consumer Requests

7021 Timeline for Responding to Requests

(b) We are concerned that validation of requests due to missed calls or lack of response to emails may take a significant amount of time. While we appreciate the provision allowing up to 90 days, it’s conditioned upon the business providing a consumer an individual notice and explanation of the reason an additional 45 days is required. This is overly burdensome especially in instances where the delay is no fault of the business. We request the 45-day timeline start after validation is complete, while still permitting an additional 45-day extension if the business provides the appropriate notice and explanation.

7022 Right to Delete

(d) The language allowing a business to delay compliance with a request to delete if data is stored on an archive or backup is welcome, however the requirement that the business apply a request to delete when an archived or backup system becomes active, is too administratively burdensome. A company could for example find itself out of compliance when data is restored years after the fact for a non-business purpose like internal audits or responding to litigation. We request that this standard become a two-part test in line with the current language. The personal information must be restored to an active system **and** next accessed or used for a sale, disclosure, or commercial purpose.

7023 Requests to Correct

(c)(2) As above we believe Business M should only have to respond to a request to correct when personal information is restored to an active system **and** next accessed or used for a sale, disclosure, or commercial purposes.



7024 Requests to Know

(i) We believe that the language detailing what a service provider or contactor must provide a business in responding to a request to know is overly prescriptive. We propose that the last clause of the sentence be stricken and the paragraph just state that the service provider or contractor must provide assistance.

7025 Opt-out Preference Signals

General Comment: This section lists standards for non-frictionless and frictionless processing of signals relating to the right to opt-out. However statutory language in 1798.135(b)(1) provides for the frictionless processing of preference signals as a means of both opting-out a consumer from the sale-sharing of their Personal Information **and** limiting the use-disclosure of their sensitive Personal Information. We are requesting clarification whether the standards for frictionless and non-frictionless signal processing in Section 7025, **can also be applied to the right to limit in Section 7027?** As the regulations are currently drafted, we believe that it is ambiguous what standards must be met to utilize frictionless signal processing of requests to limit

(a) According to the language of the regulations the purpose of the opt-out preference signal is to provide a simple and easy-to-use method to automatically opt out of sale/sharing of data. However, the language in this section appears to require all “businesses” as defined in the CCPA to process opt-out preference signals, regardless of whether they actually sell or share personal information. As drafted this regulation would require a business with gross annual revenue of over \$25 million that collects consumer personal information to process such a signal even if the business does not sell or share data. This is unnecessarily burdensome, and we request the regulations clearly exempt businesses that do not sell or share data.

(e) We believe the draft language in this section misinterprets the mechanics of Civil Code section 1798.135(b). The draft regulations note that the statute “does not give the business the choice between posting the above-referenced links or honoring the opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner.” However, section 1798.135(b)(3) provides that “[a] business that complies with subdivision (a) is not required to comply with subdivision (b)” and that “a business may elect whether to comply with subdivision (a) or subdivision (b).” This language clearly states that meeting the requirements of Section 1798.135(a) (through one or more links) exempts a business from processing opt-out preference signals under Section 1798.135(b). The statute does not *require* opt-out preference signals to be processed. As drafted, proposed section 7025(e) tacitly reads a net new requirement (processing preference signals) into 1798.135(a) or, alternatively, it reads 1798.135(b)(3) out of the statute entirely. To give meaning to the statute as written, we urge the Agency to preserve the option of posting the above-referenced links in lieu of processing preference signals, frictionlessly or non-frictionlessly.

7026 Requests to Opt-Out of Sale/Sharing

(f) This provision requires businesses to notify all third parties to whom the business has shared a consumer’s personal information after the consumer opts out of sale/sharing. We are concerned that



this provision does not make sense in the context of cross-context behavioral advertising where the opt-out will be almost instantaneous and occur on a technological level. For example, cross-context advertising cookies/pixels will stop being deployed to the user when they opt out, and the sharing with third parties will stop. In this context we think the requirement to have to inform third parties about the opt out does not make sense and it should be sufficient to actually opt out the consumer from cross-context behavioral advertising on the business's website, and stop sharing the consumer's personal information with third parties for cross-context behavioral advertising purposes. The goal appears to be to stop showing the consumer ads based on their activities across websites, and therefore there is no added benefit to having to formally notify third parties in this context.

7027 Requests to Limit Use and Disclosure of Sensitive Personal Information

(a) We ask that the agency define a "heightened risk of harm" to consumers as it relates to the use or disclosure of sensitive personal information.

Article 4: Service Providers, Contractors, and Third Parties

7050 Service Providers and Contractors:

(c) We are requesting clarification on the applicability of this paragraph. We believe that the language could be read to altogether prohibit entities from entering into contracts for the purpose of cross-context behavioral advertising, when we believe the intent is to actually clarify that contracts for cross-context behavioral advertising are always treated as contracts with third parties.

Article 5 Verification of Requests

7063 Authorized Agents

General Comment: For financial institutions that collect a variety of consumer data with varying sensitivity subject to varying laws and regulations, we believe that this class of business should be permitted to take a risk-based approach to processing authorized agent requests to minimize the risk of unintentional release of consumers sensitive personal information. Regarding a request to know, it is entirely plausible that a consumer would give an authorized agent permission to submit CPRA requests on their behalf with the intention of having that agent help the consumer understand what data is held by different companies, but the consumer would not necessarily want the third party to access sensitive personal information. We believe financial institutions must have explicit authorization in the regulations to process authorized agent request for CCPA data in a way that minimizes the risk of release of sensitive information, and does not provide a backdoor for malicious actors

(b) As currently drafted the language in this paragraph does not provide a clear mechanism for businesses, but of particular importance, financial institutions, to verify that a consumer has provided the authorized agent with a power of attorney. We have very strong concerns that this language could result in unauthorized disclosure of financial information. Therefore, we request clarification that the authorized agent in the context of subsection (b) must provide evidence of a power of attorney pursuant to Probate Code sections 4121 to 4130.



Article 8: Training and Record Keeping

7102 Requirements for Businesses Collecting Large Amounts of Personal Information

(a) We are requesting clarification on the number of consumers that trigger reporting requirements. Is the reference to 10 million consumers a reference to Californian consumers, consumers in the United States or consumers globally?

Conclusion

The life insurance industry generates approximately 225,600 jobs in California, including 81,500 direct employees and 144,100 non-insurance jobs. There are 417 life insurers licensed to do business in California and 11 are domiciled in the state. California residents have \$3.7 trillion in total life insurance coverage. State residents own 10 million individual life insurance policies, with coverage averaging \$244,000 per policyholder. And \$38 billion was paid to California residents in the form of death benefits, matured endowments, policy dividends, surrender values, and other payments in 2016 with \$8 billion in annuity benefits paid in the state in the same year.

Not only is our industry a robust contributing member of the California economy, we are proud of the fact that the financial services industry has traditionally been a conscientious and responsible guardian of customers' highly vulnerable personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades.

As stated previously, we encourage CPPA to continue to look towards existing well tested formats for compliance that would make notices more understandable. We think there are numerous areas as highlighted above where the regulations should be simplified and clarified to facilitate company compliance and, more importantly, enhance consumer clarity. And, importantly, as we indicated earlier, adequate time for compliance must be provided. We believe that businesses should have at least 1 year to build out their compliance systems from the date the regulations are adopted. Lastly, we encourage this agency to move forward as expeditiously as possible with rulemaking on cybersecurity audits, risk assessments and automated decision-making technology. It is critically important that businesses understand as soon as possible, with a delayed compliance date, the practical effect of the entire body of CCPA regulations.

Thank you, in advance, for your consideration of our comments. We would be happy to answer any questions.

Sincerely,

John W. Mangan
Regional Vice President, State Relations
American Council of Life Insurers

Matthew R. Powers
Vice President
Association of California Life and Health Insurance Companies

From: **Nick Chiappe** [REDACTED]
 To: **Regulations** <Regulations@cpga.ca.gov>
 Subject: Updated: CTA Comments on CPPA's Proposed Regulations
 Date: 23.08.2022 18:16:58 (+02:00)
 Attachments: CTA Comments on CPPA proposed regs 08.23.22.pdf (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,

Please find attached updated comments from the California Truck Association (CTA) on CPPA's Proposed Regulations. Please disregard previously submitted comments and refer to the current comments attached to this email.

Thank you,
 Nick



Nick Chiappe | Government Affairs Associate
California Trucking Association
 4148 East Commerce Way
 Sacramento, CA 95834
 C: [REDACTED] | E: [REDACTED]
 W: www.caltrux.org



A one-stop-shop for all things testing? Your search is over.

Visit www.TSCtesting.com or email Karina Fernandez at [REDACTED] to learn more.



August 22, 2022

Via Email to: regulations@cpha.ca.gov

California Privacy Protection Agency
Attn: Brian Souplet
2101 Arena Blvd., Sacramento, CA 95834

Re: CTA Comments on the Proposed Regulations by the CPPA

Dear Board Members of the CPPA,

The California Trucking Association (CTA) appreciates the opportunity to submit comments to the CPPA's July 8th draft of proposed regulations on consumer data privacy. The CTA promotes leadership in the California trucking industry, advocates sound transportation policies to all levels of government, and works to maintain a safe, environmentally-responsible and efficient California transportation goods movement system.

As we stated in our [previous letter](#) to the Attorney General on November 14, 2019, classifying a transportation/logistics company as a "service provider" for data privacy purposes imposes outsized burdens on our industry in light of the unique regulatory and legal environment in which we operate. In addition, such a classification improperly discounts the fact that our member companies are public facing "businesses" with direct consumer relationships in their own right.

Therefore, we request the following amendments to Section 7050(b) of the July 8th proposed regulations put forth by the CPPA.

Amending the Substantive Text

In Section 7050(b):

"A shipping service provider that delivers businesses' products to their customers may use *and retain* the addresses obtained from their business clients and *its* experience delivering to those addresses *for legitimate business purposes permitted under applicable laws, including to comply with laws*, to identify faulty or incomplete addresses, ~~and thus,~~ or *to* improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers."

Amending the Placement of the Text

In addition to the requested amendment above, we ask that the above-captioned paragraph in its entirety be moved from Section 7050(b) to a new Section 7002(b)(5). Such a move would make for a cleaner fit for two reasons: first, since Section 7002, in general, deals with restrictions on the collection and use of Personal Information, the above-captioned paragraph in a new Section 7002(b)(5) would be an appropriate way to illustrate the more specific principles of purpose limitation and data minimization; second, the proposed new Section 7002(b)(5) would immediately follow Section 7002(b)(4), which deals with a similar hypothetical involving delivery companies.

Why A “Service Provider” Designation is Problematic for Transportation/Shipping Companies

A “service provider” designation will create operational issues for shipping companies and the package transportation industry. Retailers and corporate customers continue to insist that carriers and shipping companies are their “service providers” under the CCPA and subject to their controls, which precludes shipping companies from using shipping data for legitimate business purposes. Allowing shipping companies to be designated as a “business” will ensure the free flow of goods, while still protecting the privacy rights of consumers.

Contents of the Package:

Shipping companies do not act as a “data controller/business” or a “data processor/service provider” with regard to information that may be contained in the packages they transport. That rationale is straightforward: shipping companies have no control over the contents, nor do they know whether personal data is contained within. These shipping companies merely act as a conduit of that personal data, without exercising any actual control over it. For a more detailed discussion of mail delivery services and their status, you may refer to the guidance from the Dutch regulator at <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht> and UK Data Protection Regulator (ICO), at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (¶¶ 33-39).

Shipping Label Data:

Shipping companies act as a “data controller/business” for data on the Shipping Label and data necessary to provide our track and trace service, and not a “data processor/service provider” on behalf of a “business.” This position is also consistent with guidance from various European data regulators and ICO’s document referenced above. For example, the Bavarian data authority’s guidance, available at https://www.lida.bayern.de/media/info_adv.pdf, gives examples that demonstrate that, in some contexts, the transfer of personal data is an “unavoidable accessory” (unvermeidliches “Beiwerk”) (p. 3-4). The examples that are provided include courier services, cleaning services, and repair and maintenance work. These examples make clear why the transfer of personal data can be ancillary to the services provided: one has to give one’s address to the cleaner to have clothes returned or give vehicle information to the mechanic to have it worked on and give names and addresses to the courier to have a package delivered. But these

providers should not be classified as “data processors/service providers” as far as the data protection laws are concerned.

The California privacy laws have placed significant restrictions on “service providers” with respect to how they can use the data. For example, the CPRA Regulations “[prohibit]s the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations.” Section 7051(a)(3). The Regulations also state that “the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.” Section 7051(a)(9). The Regulations also provide that “the service provider or contractor [must] provide the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers’ requests made pursuant to the CCPA.” Section 7051(a)(6).

The practicalities for and legal requirements imposed on shipping companies demonstrate why they must be “businesses” and not “service providers.” If one sends a box to John Smith at 123 Main Street, shipping companies have John Smith at 123 Main Street in its database. If shipping companies agreed to be a “processor/service provider,” they would be obligated to only use John Smith at 123 Main Street in accordance with instructions from a business and would be obligated to delete data if asked by a business. This, however, poses a direct conflict with regulatory requirements for shipping companies that must retain certain shipping records (e.g., customs and U.S. Department of Transportation requirements that require certain records be kept, Federal Aviation Regulations that require airlines to check the “do not fly” list, etc.).

Additionally, when a business asks to have a name and address deleted, that poses a particular hardship for shipping companies because that name and address are not uniquely associated with any single shipping customer. John Smith might be a customer of another retailer who ships, or he might be a customer of the shipping company himself. John Smith may no longer want a particular retailer to hold his personal data, but that does not mean he wants the shipping company to delete his data and no longer be able to receive tracking updates of other packages he has bought from separate retailers. Shipping companies could not restrict processing or delete that data because it does not belong to any particular business.

Likewise, an address deletion request from a data subject will prove difficult. For example, John Smith may make a request to have 123 Main Street deleted from a shipping company’s records, but 123 Main Street is not only associated with him. There may be family members that live at 123 Main Street, or John Smith may have moved and 123 Main Street may now be the residence of another individual. Accordingly, shipping companies should be considered a “business” in their own right and have more discretion than a “service provider” when it comes to how personal data is processed in furtherance of individual privacy rights.

Importantly, if shipping companies are considered “businesses,” rather than “service providers,” with respect to the personal data such companies obtain as part of their business, such a classification does not adversely affect the protection of such data. Shipping companies, like all other businesses, would still need to demonstrate that they have proper security safeguards and procedures in place to ensure the protection of all individuals’ personal data they process.

For these reasons, we urge you to classify transportation and/or shipping companies as a “business,” not a merely a “service provider.” As a way to clarify that distinction while still

protecting consumer data, we respectfully ask for the text of Section 7050(b) be amended and moved to a new Section 7002(b)(5), as detailed above.

Sharing Data with Package Transportation Companies to Ship Packages Should Not be Deemed a “Sale” of Personal Information.

CTA respectfully submits that it is critical to the package transportation industry to confirm that retailers and other corporate customers do not “sell” Shipping Information when they provide that information to transportation providers. This clarification is critical, due to the scope of the definition of “sell” in the CCPA, because transportation providers inherently use Shipping Information for more than simply to deliver each individual package to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, “drop boxes” where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.
- Shipping Information constitutes a combination of information received from customers, plus information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.
 - Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight (“DimWeight”) or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier’s package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.
 - One of the more prominent examples of this is addresses: annually, carriers often correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

The use of Shipping Information by transportation providers beyond the simple delivery of each individual package to each individual address, when requested not by the individual consumer but by a retailer or other corporate customer, could therefore be considered to result in a sale of that information by the retailer to the carrier, but for the exception in Cal. Civ. Code Section 1798.140(ad)(2)(A) (operative Jan. 1, 2023).

- Subsection 1798.140(ad)(2)(A) provides that a business does not “sell” personal information when consumers “direct the business to . . . intentionally disclose personal information.” This is precisely what happens when consumers order goods from carriers’ corporate customers that need to be shipped.
- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, retrieving the merchandise from the corporate customer’s facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.
- To exempt consumer-directed data disclosures from being a “sale,” the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the Section 1798.140(ad)(2)(A) requires only that the consumer “direct” a retailer or manufacturer to “intentionally disclose” their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

Shipping Information remains protected under the CCPA in the hands of the carrier. Carriers are businesses that determine the purposes and means of the processing of Shipping Information and must comply with the CCPA, including the various privacy obligations and protections established by the statute. This information is also protected by a longstanding federal law that regulates its handling and disclosure.¹

CTA believes the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a “sale” pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as “service providers” as defined in the CCPA, out of a concern that disclosing data to a separate “business” carries a “sale” risk. This designation would prevent package transportation providers from being able to use Shipping Information for any purpose beyond delivering each individual package – a result that will impair operations across the industry with no corresponding consumer benefit. CTA therefore respectfully requests the CPPA to clarify the application of Section 1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CPPA’s rulemaking authority under Cal. Civ. Code Section 1798.185(b).

The Clarifications Requested by CTA are also Consistent with the Law under the European Union General Data Protection Regulation, which Provides that Package Transportation Providers Are Controllers, not Processors, as to Shipping Information.

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR,

¹ See 49 U.S.C. § 14908.

package transportation providers are deemed controllers that have the right to determine the purposes and means of the processing of Shipping Information.

- As the members of the CPPA will be aware, the definition of “controller” in the EU is analogous to the definition of “business” in the CCPA, in that both a controller and a business “determine[] the purposes and means” of the processing of personal information. Cal. Civ. Code Section 1798.140(c)(1); GDPR Art. 4(7). The GDPR also contains the concept of a “data processor”, which, similar to a service provider under the CCPA, is defined as an entity that processes data on behalf of a controller.
- European regulators who have addressed the issue have consistently found that package transportation companies are best classified as “controllers,” not as “processors.” As an example, the United Kingdom’s Information Commissioner’s Office issued guidance in 2014 stating that a delivery service “will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking ... such as individual senders’ and recipients’ names and addresses.”² More recently, the Bavarian Office for Data Protection Supervision issued 2018 guidance stating that “postal services for letter or package transportation” are generally “not data processing,” but instead “specialized services” offered by “an independent controller.”³

We respectfully suggest that the European practice reflects a recognition of the fundamental, inherent, and accepted purposes for which package transportation providers must use personal information to perform their daily operations at the level expected by both consumers and customers. We request the CPPA to take a similar approach under the CCPA by clarifying the application of Section 1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CPPA’s rulemaking authority under Cal. Civ. Code Section 1798.185(b).

The CPPA Should Establish Reasonable Processes for Handling Employee Privacy Requests.

The CCPA as originally drafted applied equally to personal information concerning traditional “consumers” and employees. To address this apparent drafting error, the legislature amended the statute to exclude employee personal information used solely in the context of the employment relationship except with respect to the requirement to provide a notice at collection, and the private right of action for certain data security incidents. Cal. Civ. Code Section 1798.145(h)(1). The California Privacy Rights Act retained this limited exemption, but provides that it will expire as of January 1, 2023, subjecting employee personal information to the full panoply of the CCPA’s consumer privacy standards on and after that date. Cal. Civ. Code Section 1798.145(n)(3) (operative Jan. 1, 2023).

This means that, among other things, employers will have the obligation to process and fulfill requests to know, for specific pieces of information, to correct, and to delete submitted by their

² See Information Commissioner’s Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

³ See Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DS-GVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and Processors]] at 2 (July 20, 2018), available (in German) at https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

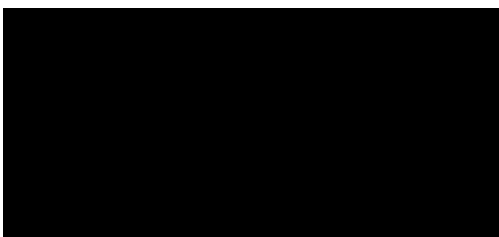
California workforce. CTA is concerned about the significant new regulatory burden these standards will impose on our members for several reasons:

- Requiring employers to identify, review, and deliver copies of all personal information held about employees will require employers to expend significant new resources, through dedication of personnel and purchases of technology, to locate, catalog, process, and transmit vast new volumes of personal information in electronic and paper form. Much of the personal information businesses retain about employees is “unstructured,” difficult to locate, difficult to search, and created by the employee herself. Employers will also have an obligation to review this information carefully before producing it back to the employee to ensure the protection of other employees who may be identified or identifiable from the data.
- The right to specific pieces of information goes beyond even the rights of employees in litigation. There, discovery requests and compulsory process are at least bounded by discoverability standards and subject to judicial oversight.
- We anticipate requests to know, for specific pieces of information, and to delete will therefore primarily become litigation or pre-litigation tools, not mechanisms for employees to realize important privacy interests.

CTA therefore respectfully requests the CPPA to exercise its rulemaking authority under Cal. Civ. Code Section 1798.185(b) to clarify that the obligation of employers to produce information in response to a request for specific pieces of information is limited to categories such as worker contact, job title and duties, emergency contact, and salary information. We further request that the CPPA clarify that employers may afford reasonable self-service options for employees to request and receive copies of applicable information in response to a request.

We thank you for your consideration of these requests as your agency moves through the rulemaking process on this important issue.

Sincerely,



Chris Shimoda
Senior Vice President of Government Affairs



From: Robyn Mohr [REDACTED]
To: Regulations <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 18:41:13 (+02:00)
Attachments: NMA CPPA Proposed Regulations Comments (8.23.22).pdf (13 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find the CPPA Public Comment from the News Media Alliance.

Robyn Mohr (She/Her)

Senior Counsel



901 New York Avenue NW, Suite 300 East | Washington, DC 20001

Direct Dial: [REDACTED] | **Mobile:** [REDACTED] | **E-mail:** [REDACTED]

Los Angeles | New York | Chicago | Nashville | Washington, DC | Beijing | Hong Kong | www.loeb.com

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify the sender. Please destroy the original transmission and its attachments without reading or saving in any manner. Thank you, Loeb & Loeb LLP.



August 23, 2022

regulations@coppa.ca.gov

California Privacy Protection Agency

Attn: Brian Soublet

2101 Arena Blvd.

Sacramento, CA 95834

Re: Comments of the News Media Alliance in Response to the California Privacy Protection Agency’s Notice of Proposed Rulemaking Issued with the Office of Administrative Law on July 8, 2022

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. The free press is on the front lines helping the American people hold accountable those in positions of power within our democracy and around the world. A vibrant and financially stable independent press is therefore essential to a healthy democracy. The News Media Alliance (the “Alliance”) is a nonprofit, non-stock corporation organized under the laws of the commonwealth of Virginia. It has no parent company. The Alliance represents news and media publishing associations, including nearly 2,000 diverse news and magazine publishers in the United States—from the largest nationally and internationally recognized organizations to hyperlocal news sources, from digital-only and digital-first to print news. Alliance members account for nearly 90% of the daily newspaper circulation in the United States. The Alliance is also the industry association for close to 100 magazine media companies with more than 500 individual magazine brands, that cover news, culture, sports, lifestyle, and virtually every other interest, vocation or pastime enjoyed by Americans. The Alliance diligently advocates for news organizations and magazine publishers on a broad range of issues that affect them today.

The Pew Research Center reported that, “the total combined print and digital circulation for locally focused U.S. daily newspapers in 2020 was 8.3 million for weekday (Monday-Friday) and 15.4 million for Sunday.”¹ Digitally, in the fourth quarter of 2020, the top 50 newspapers saw almost 14 million unique visitors each month. In addition, there are on average more than 220 million magazine readers in the U.S. each year. Digital advertising is a significant source of revenue for these news and media outlets, large and small, and significantly helps keep the press (i) free from government control, (ii) affordable and accessible to all (not just to those who can afford a subscription), and (iii) at the highest level of integrity the people of the United States (and the world) have come to depend on. A thriving and free press has never been more important to American democracy. With a well-designed privacy law, the press can continue to do its job as intended in the U.S. Constitution, and consumers can continue to have access to cost-efficient and reliable news and media sources, while retaining control of the processing of their personal information.

The California Privacy Protection Agency (the “Agency”) proposed regulations (“Regulations”) promulgated pursuant to the California Privacy Rights Act (“CPRA”), which amended the California Consumer Privacy Act of 2018 (collectively with the CPRA, the “CCPA”) and is effective January 1, 2023.

¹ See, “*Local Newspapers Fact Sheet*” by Katerina Eva Matsa and Kirsten Worden, available at <https://www.pewresearch.org/journalism/fact-sheet>.

The California Privacy Protection Agency Board (the “Board”) approved the proposed Regulations and the Board filed a Notice of Proposed Rulemaking with the Office of Administrative Law on July 8, 2022. While the Regulations are helpful on a number of levels, they impose certain additional burdens on news and media organizations that will make compliance increasingly difficult, provide no added benefit to consumers, and fail to consider the implications of the employee and business relationship exemptions that expire January 1, 2023.

The Alliance believes in giving consumers more transparency and control regarding the collection, use, and sharing of their personal information. The Alliance also supports clear and consistent rules that align with other privacy laws and that support practical implementation and operationalization by news publishers of all sizes across digital and offline media, regardless of jurisdiction.

The Alliance respectfully submits the following comments on certain topics (designated below) in response to the California Privacy Protection Agency’s Notice of Proposed Rulemaking issued with the Office of Administrative Law on July 8, 2022.

I. The Agency Must Clarify the Scope of Protection for Journalism Set Forth in the CCPA.

The First Amendment to the U.S. Constitution and the California Constitution² protect a free and independent press. The text of the CPRA explicitly recognizes these constitutional protections by exempting those engaged in noncommercial journalism activities from the CCPA requirements:

The rights afforded to consumers and the obligations imposed on any business under [the CCPA] shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article 1 of the California Constitution.³

The freedom of the press is protected under federal and state law, and should not be hindered by the inability of news and media outlets to engage in newsgathering activities or share information with those assisting in the creation and distribution of vital information to the people.

The Alliance asks the Agency (as within its power under the CCPA to establish “any exceptions necessary to comply with state or federal law”⁴) to make explicit in the Regulations that “selling” and “sharing” does not include conduct by those engaged in journalism or newsgathering, as those activities are inherently noncommercial. In other words, the Regulations should make clear that renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating (orally, in writing, or by electronic or other means), a consumer’s personal information by a news media outlet to another business or to a third party in support of journalism is not “selling” or “sharing” under the CPRA provided that the

² California Constitution Art. I, §2.

³ Cal. Civ. Code §1798.145(l). Section 2(b) of Article I of the California Constitution states as follows: “A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or a by a press association or wire service, or any person who has been so connected or employed, shall not be adjudged in contempt by a judicial, legislative, or administrative body, or any other body having the power to issue subpoenas, for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public.”

⁴ Cal. Civ. Code §1798.185(a)(3).

provisions of the CPRA are otherwise complied with (e.g., providing an accurate privacy policy and implementing reasonable security procedures and practices).

In addition, the Regulations should make explicit that, for purposes of fulfilling the intent of Section 1798.140(ag), all agreements between news media outlets and their vendors, even for purposes such as cross-contextual behavioral advertising, should be viewed as contracts with “service providers” for a “business purpose” and not subject to 11 CCR §7050(c),⁵ provided that the vendor is otherwise prohibited from using that personal information other than as explicitly set forth in the agreement with the news media outlet, and not for any secondary purposes.

II. The Agency Should Provide Further Clarification on How to Properly Post Links Required under the CCPA and Regulations for Mobile Applications.

The Regulations provide that for mobile applications, links must be accessible within the mobile application.⁶ The Regulations also require that the link to the privacy policy be on the platform page or download page of the mobile application,⁷ the download or landing page of a mobile application,⁸ and in the application’s menu settings.⁹ The notice at collection may be provided through a link to the notice on the mobile application’s download page and within the application, such as through the application’s settings menu.¹⁰

From an operational standpoint, these requirements are problematic because many mobile applications have limited space and mobile applications do not typically have footers, like many websites viewed on a mobile device. In addition, App Stores tend to place strict limitations on how, what, and where businesses can link to and from the mobile application’s download page. Often times, the links to the privacy policy and other applicable notices are found in a “hamburger” menu or gearbox, which consumers have come to learn is an easily accessible location for important additional information.

Given these consumer expectations, and the fact that the Regulations dictate that all links required under the CCPA and Regulations be accessible via a privacy policy available to consumers on the mobile application download page,¹¹ the Alliance requests that the Agency clarify that if the required links are placed in the privacy policy and in the mobile application’s hamburger menu or gearbox, they will be deemed “conspicuously placed” for purposes of the CCPA and the Regulations.

⁵ 11 CCR §7050(c). “A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers.”

⁶ 11 CCR §7003(d). “For mobile applications, a conspicuous link shall be accessible within the application, such as through the application’s settings menu. It shall also be included in the business’s privacy policy, which must be accessible through the mobile application’s platform page or download page.”

⁷ *Id.*

⁸ 11 CCR §7011(d).

⁹ *Id.*

¹⁰ 11 CCR §7012(c)(3).

¹¹ 11 CCR §7003(d).

Accordingly, the Alliance recommends the following revisions to 11 CCR §7003(d) to align with the language in 11 CCR §7003(c) and to clarify the placement of these links:

For mobile applications, a conspicuous link **required under the CCPA or these regulations** shall be accessible within the application, such as through the application's settings menu- ~~It shall also be included in, and~~ in the business's privacy policy, which must be accessible through the mobile application's ~~platform page or~~ download page.

All other references to the location of required links and notices with respect to mobile applications, including within the privacy policy, should either be removed or revised to align with the recommended language above. This will help provide uniformity across websites and among mobile applications such that consumers will know exactly where to look for privacy-related notices, no matter which format a consumer chooses to interact with the business.

III. The Agency Should Not Restrict a Service Provider's or Contractor's Ability to Use Information Collected from One Business for its Own Consumer-Friendly Business Purposes.

Businesses (and their service providers and contractors) should be able to combine personal information from different sources for legitimate business purposes. The Alliance submits that the Regulations should permit uses of personal information by service providers in ways that promote consumer privacy, even if that involves the combination of information from different sources and/or the use of information to provide services to more than one business.

The Regulations provide:

A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except...[f]or internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person.¹²

This provision would severely impact publishers' ability, for example, to use any service provider or contractor that provides analytic services to a publisher. Many technology service providers use a common data point (such as an IP address), received from multiple businesses, to provide services to many different businesses, to the benefit of consumers. For example, frequency capping or sequencing functions are extremely helpful to consumers because they limit the number of times consumers may see the same advertisement on a publisher's site. Service providers and contractors are only able to bring this benefit to consumers if they are able to take the information they receive from other similarly-situated businesses, and use that information collectively.

The Alliance recommends the following revision to 11 CCR §7050(b)(4):

For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person **unless the service provider or contractor is using the information solely for a business purpose that is disclosed in the business's privacy policy, to consumers when fulfilling a request to know, and in the contract with the service provider or contractor.**

¹² 11 CCR §7050(b)(4).

IV. The Regulations Should Provide Further Guidance on the Requirements for Opt-out Preference Signals.

A. The Definition for “Frictionless Manner” Should Acknowledge Opt-Out Preference Signal Limitations.

The Regulations provide:

In lieu of posting the “Do Not Sell or Share My Personal Information” link, a business may provide an alternative opt-out link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a notice of right to opt-out of sale/sharing in accordance with these regulations.¹³

However, what constitutes a “frictionless manner” under Section 7025(f) and (g) does not consider that opt-out preference signals, at least with their current technical capabilities, are virtually incapable of effectuating an opt-out in a “frictionless manner.” It most certainly cannot be “frictionless” for traditional offline services, such as the content provided by print news and magazine publishers. Indeed, the very concept of the opt-out preference signal was to opt consumers out of cross-context behavioral advertising across browsers. No single opt-out preference signal, including the Global Privacy Control, can provide a one-stop-shop for consumers to opt out of all sales and sharing for cross-context behavioral advertising, much less to limit the use of sensitive personal information. Meeting the Agency’s definition of “frictionless manner” in online and offline contexts is impossible without forcing businesses to digitally combine all the information it could possibly have on a person, into a single database. It is hard to imagine that even the original drafter of the CCPA would want businesses to build massive databases, simply to meet the “frictionless manner” standard set forth in the Regulations.

Further, as the Regulations are currently drafted, providers of opt-out preference signals are not required to disclose these limitations to consumers, leading consumers to believe the opt-out preference signals can and will do more than is actually possible. Respectfully, it would be extremely harmful for consumers to be told opt-out preference signals are an easy one-stop fix, when in reality it is anything but that. The Agency should reconsider the definition of “frictionless manner” to account for the technical limitations of opt-out preference signals. Considering the fact that additional methods to opt-out must be provided in a privacy policy and that notices of the right to opt-out have to be provided in the same manner in which the business collects personal information that it sells or shares (e.g., offline, through a connected TV, etc.),¹⁴ the Alliance recommends the following revision to 11 CCR §7025(g)(3):

Allows the opt-out preference signal to fully effectuate the consumer’s request to opt-out of sale/sharing **to the extent the business is able to effectuate the opt-out across browsers, devices, and offline databases based on the consumer information relayed to the business by the opt-out preference signal.** For example, if the business sells or shares personal information offline and needs additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales or sharing of personal information, then the business has ~~not~~ fully effectuated the consumer’s request to opt-out of sale/sharing **to the extent it complies with the (i) opt-out preference**

¹³ 11 CCR §7013(d).

¹⁴ 11 CCR §7013(e)(3).

signal for sales/sharing associated with the personal information provided to the business by the opt-out preference signal and (ii) with the other obligations set out in 7025(f) and (g).¹⁵

B. Providing Confirmation of Compliance with Opt-Out and Limit the Use Requests Should be Optional.

The Regulations provide:

A business shall comply with a request to opt-out of sale/sharing by...[p]roviding a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business.¹⁶

The Alliance asks the Agency to recognize that this poses a significant burden on businesses without the technological, financial, and/or employee resources to build and properly effectuate compliance with this obligation. As such, the Alliance respectfully requests that the Agency make this optional until implementation is more feasible for businesses across the board.

V. Businesses Should Have 45 Days to Respond to a Request to Limit the Use of Sensitive Personal Information From the Date It Was Received.

The Regulations provide:

A business shall comply with a request to limit by...[c]easing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.¹⁷

For many businesses, the sale/sharing of personal information is limited to what is collected through various tracking technologies permitted to collect information from the website or mobile application. As such, a request to opt-out of the sale/share of personal information can be complied with by preventing the collection of information from those tracking technologies. The same cannot be said for the collection of sensitive personal information, simply by the nature through which sensitive personal information is received. Sensitive personal information is generally not collected by tracking technologies but manually inputted or uploaded by the consumer. As a result, complying with requests to limit the use and disclosure of sensitive personal information may take more human effort to effectuate versus a request to opt-out of the sale/share of personal information. This is true regardless of the fact that requests to limit do not need to be verified.

To address these operational complexities and to bring the consumer's right to limit sharing their sensitive personal information in line with the timeline for other consumer rights, the Alliance recommends that the Regulations provide businesses 45 calendar days to respond to a consumer's request to limit the use of sensitive information.

The Alliance recommends the following revision to 11 CCR §7027(g)(1):

¹⁵ 11 CCR §7025(g)(3).

¹⁶ 11 CCR §7026(f)(4).

¹⁷ 11 CCR §7027(g)(1).

A business shall comply with a request to limit by...[c]easing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than ~~45~~ **business calendar** days from the date the business receives the request.

VI. The Obligation to Notify Third Parties of Opt-Out and Deletion Requests Exceeds the Scope of the Agency's Rulemaking Authority and Should be Eliminated.

The Regulations provide:

A business shall comply with a consumer's request to delete their personal information by...[n]otifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.¹⁸

and

A business shall comply with a request to opt-out of sale/sharing by...[n]otifying all third parties to whom the business makes personal information available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises, that the consumer has made a request to opt-out of sale/sharing and directing them 1) to comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period. In accordance with section 7052, subsection (a), those third parties and other persons shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.¹⁹

These proposed Regulations are problematic as they would require retroactive application of the do not sell and deletion obligations and thereby exceeds the scope of the Agency's power to regulate. "New statutes are presumed to operate only prospectively absent some clear indication that the Legislature intended otherwise." *Elsner v. Uveges*, 34 Cal. 4th 915, 936 (2004). Here, there is no clear indication that the Legislature intended the do not sell and deletion obligations to apply retroactively. Moreover, the statute only requires a prospective obligation on businesses that honor do not sell requests.²⁰

Second, businesses are not always in a position to push these obligations onto third parties. As the Agency is aware, often the biggest players within the ad tech ecosystem are unwilling to negotiate terms with other businesses. Even the most well-known companies, with actual bargaining power in most situations, are unable to negotiate contractual terms with vendors that comply with the CCPA and allow the businesses to flow down those obligations. Even where self-regulatory organizations have developed frameworks for compliance purposes, there is no guarantee that businesses can obligate third parties to comply for the same

¹⁸ 11 CCR §7022(b)(3).

¹⁹ 11 CCR §7026(f)(3).

²⁰ Cal. Civ. Code §1798.135(c)(4). "For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations."

reasons stated above. At the same time, these parties are still an essential and necessary part of the online ecosystem and the Alliance respectfully asks the Agency to acknowledge the positions taken by these essential vendors.

In order to avoid any retroactive application of the CCPA and to address the reality that businesses, especially small businesses, are almost never in a position to push obligations on third parties, the flow down obligation to third parties should be eliminated or a more practical approach should be adopted. For example, the Agency should require businesses to flow down the requests but not be responsible for the third party's compliance with those requests, regardless of whether it has actual knowledge that the third party is not complying with such requests, where the business was unable to negotiate more favorable terms.

VII. The Agency Should Increase the Number of Consumers that Would Trigger Metrics Reporting for Businesses.

The Agency has maintained explicit metrics reporting requirements for a business that “alone or in combination, buys, receives for the business’s commercial purposes, sells, shares, or otherwise makes available for commercial purposes, the personal information of 10,000,000 or more consumers...”²¹

It is understandable that the Agency and consumers would benefit from such metrics reporting, particularly from businesses that process large amounts of data. However, the 10,000,000 consumer threshold is a low threshold in today’s digital world and will trigger reporting requirements for many small and local publications who simply may not have the resources to fulfill this additional obligation.

The Alliance strongly recommends that the Agency consider increasing the consumer threshold that would trigger this metrics reporting obligation so that those reporting obligations truly apply to the businesses collecting large amounts of personal information. Accordingly, the Alliance believes that the “10,000,000 or more” consumer threshold should be increased to 40,000,000 or more consumers.

VIII. The Agency Should Enumerate Additional Business Purposes For Which Service Providers and Contractors Can Use Information It Collected On Behalf of a Business.

The Regulations enumerate certain uses for which a service provider or contractor may use personal information that it has collected on behalf of a business.²² However, service providers and contractors need the flexibility to make other uses of such information for their own business purposes. For example, the Regulations only permit service providers and contractors to use such personal information “[f]or the specific business purpose(s) and service(s) set forth in the written contract required by the CCPA and these regulations” and “[f]or the purposes enumerated in Civil Code Section 1798.145, subdivisions (a)(1)-(4).”²³ This language would prohibit service providers and contractors from being able to create aggregated or de-identified data from such personal information (even where the agreement between the service provider or contractor and business specify the obligations for aggregated or de-identified data), and it is unclear to the Alliance why the Agency seeks to restrict such activity.

The language would also prohibit the building of consumer profiles to use in providing services to another business and the correction and augmentation of data acquired from another source in ways that promote consumer privacy.

²¹ 11 CCR §7102(a).

²² 11 CCR §7050(b)(1)-(6).

²³ *Id* at (b)(1)-(4).

The Alliance respectfully requests that the Agency consider enumerating the following business purposes in 11 CCR §7050(b): (i) the collection, use, retention, sale, and disclosure of consumer information that is deidentified or in the aggregate, (ii) the combination of personal information from different sources to enable businesses to better understand the demographic make-up of the communities they serve, for internal business planning/benchmarking purposes. For example, publishers obtain age and gender data from a vendor to compile general statistics about the demographics of event attendees (but do not use this information to create profiles or individually target those attendees); and (iii) the combination of personal information from different sources for purposes of data hygiene. For example, publishers may use a vendor to check public databases to make sure the publisher has up to date, accurate contact information (name, mailing address, phone number) for their subscribers/users for direct marketing purposes.

IX. The Agency Should Offer Guidance On How To Contractually Restrict Vendors Who Provide Services as a Third Party and as a Service Provider and/or Contractor.

The Regulations state that if a contract is for cross-context behavioral advertising the vendor cannot be a service provider.²⁴ However, often, technology providers offer a variety of services that could make them a service provider in one context and a third party in another, depending on the services being provided.

The Alliance asks the Agency to take this business reality into consideration and clarify in the Regulations that if the contract clearly sets out where the vendor acts as a third party for cross-contextual behavioral advertising, a service provider, and/or a contractor (and includes the necessary obligations for each, as appropriate) then the vendor should be deemed as acting in the role as set out in the agreement (provided that the vendor and business process personal information according to the terms and roles of the agreement, and otherwise comply with the CCPA).

X. The Agency Should Specify Regulations For Deceased Consumers.

As noted above, the CCPA defines a consumer as “a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.”²⁵ The definition of “resident” in Section 17014 of Title 18 of the California Code of Regulations does not specify that the resident must be living.

Alliance members anticipate that households, family members, or estates, will attempt to use the consumer rights afforded in the CCPA to make requests on behalf of a decedent. The European Union’s General Data Protection Regulation, for example, explicitly confirms that data subject rights do not apply to the personal data of deceased persons.²⁶ For the sake of transparency and consistency, the Alliance recommends the Agency make explicit that the CCPA applies only to living natural persons, consistent with other consumer-focused privacy laws.

²⁴ 11 CCR §7050(c). “A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising...A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor.”

²⁵ Cal. Civ. Code §1798.140(i).

²⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Recital 27) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

XI. The Agency Should Restrict and Set Additional Obligations on Agency Conducted Audits.

The Regulations propose a broad audit right, with no restrictions or obligations whatsoever on the Agency in how it may conduct an audit. The scope of this audit right goes far beyond what is permitted by the CCPA. The Alliance respectfully submits that the Agency has failed to meet its obligation under the CCPA to issue “regulations to define the scope and process for the exercise of the agency’s audit authority, to establish criteria for selection of persons to audit, and to protect consumers’ personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.”²⁷ Pursuant to the CCPA, the Regulations should set forth an objective standard to guide the Agency’s selection of which businesses it will audit, and clarify what constitutes a “significant privacy harm” that could give rise to an audit. Without a clear and objective standard, it will be difficult for businesses to sufficiently cooperate with an audit. Further, the Regulations do not appear to protect consumer personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena. The Regulations should include requirements for technical, administrative, and physical safeguards that the Agency must follow in order to protect consumers’ personal information during the performance of the audit and to ensure that the audit is not unduly burdensome.

The Regulations provide:

[T]he Agency may conduct an audit if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law...Audits may be announced or unannounced as determined by the Agency.²⁸

The Alliance requests that the Agency set more detailed boundaries before conducting an audit and to explicitly set out the procedures for which it must follow before conducting an audit. At a minimum, the Agency should specify with detail the steps the Agency shall take before conducting an unannounced audit and how the Agency should conduct itself during any audit it conducts. Further, the Agency should explicitly set out in the Regulations that the Agency is not permitted to conduct audits under the CCPA or these Regulations until the Agency has provided “guidance to businesses regarding their duties and responsibilities under [the CCPA] and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with [the CCPA] pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.”²⁹

XII. The Agency Should Remove Violations for Unintentional Dark Patterns

The Regulations provide:

A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent.³⁰

In the Initial Statement of Reasons, the Agency takes the position that because the use of dark patterns negates any agreement for consent, the use of dark patterns does not have to be intentional, it only needs to have “the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further

²⁷ Cal. Civ. Code §1798.185(a)(18).

²⁸ 11 CCR §7304(b) and (c).

²⁹ Cal. Civ. Code §1798.199.40(f).

³⁰ 11 CCR §7004(c).

defined by regulations.”³¹ However, a dark pattern should need to be designed or manipulated with such an effect, meaning that a truly unintentional dark pattern should not rise to a violation under the CCPA. Further, upon review of the annotated CPRA amendment, the annotation states that with respect to issuing regulations on the use of dark patterns to opt consumers back into the sale/share of personal information, there should be “No *coercive efforts* to dupe consumers into opting back into the sale of their information.”³² More importantly, with respect to the use of dark patterns negating consent, the annotation to this very provision of the CPRA states, “consumers cannot compete against unlimited computing power and *intentionally-obfuscating terms & conditions, privacy policies, or interfaces.*” Clearly, the drafters of the CPRA amendment believed that the use of dark patterns involved some intention to subvert or impair user autonomy, decisionmaking, or choice on the part of the business.

Nevertheless, the Alliance recognizes that consent obtained through the use of a dark pattern, intentionally designed or not, should be invalid. However, the Alliance asks the Agency to consider that to the extent the business can show the use of the dark pattern was unintentional – for example, by proof that some internal process or review designed to remove dark pattern designs and manipulations was followed before implementation – such “unintentional” dark pattern will not amount to a violation of the CCPA if the business either (i) stops the processing of personal information for which the invalid consent was the basis of such processing; or (ii) obtains valid consent from the consumer to continue such processing.

XIII. The Agency Should Set Out Regulations Specifically for Employee Data and Business to Business Data

The Regulations do not consider the application of the CCPA or the Regulations to personal information and sensitive personal information collected in the employee or business to business (B2B) context (personal information that was previously exempt from most of the obligations in the CCPA).

The Alliance requests that the Agency, in accordance with its power under the CCPA,³³ draft Regulations that address how businesses should handle CCPA requests received from consumers in the employee or B2B context. For example, both employers and businesses operating in the B2B context process sensitive personal information in order to maintain and facilitate that relationship. The Regulations should explicitly carve out such uses from the obligation to offer the employee or the B2B consumer the right to limit the use of such sensitive personal information. Another example is the contents of a consumer’s mail, email, and text messages, unless the business is the intended recipient of the communication. Often, the business is not the intended recipient of these communications but the communications are sent *for the benefit* of the business. Consumers acting in the context of the employee or B2B relationship should not be able to limit the use of such communications by the business for its own business purposes. Processing personal information collected by a business about a consumer, where the consumer is a job applicant, employee, owner, director, officer, medical staff member, or contractor of the business should be considered a “business purpose,” to the extent that the business is processing the consumer’s information within the context of those roles and relationship. Further, the processing of personal information reflected in a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company,

³¹ Cal. Civ. Code §1798.140(l). “‘Dark pattern’ means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.”

³² See. Annotation to Cal Civ. Code §1798.185(20)(C)(iii) (*emphasis added*); available at <https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/>.

³³ Cal. Civ. Code §1798.185(a)(19)(C)(i). “The Agency shall “issu[e] regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer’s sensitive personal information, including...determining any additional purposes for which a business may use or disclose a consumer’s sensitive personal information.”

partnership, sole proprietorship, nonprofit, or government agency *and* whose communications or transaction with the business occur within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency should also be considered a business purpose.

The lack of guidance regarding the treatment of personal information and sensitive personal information collected in the employee or B2B context, imposes a significant amount of uncertainty as well as meaningful compliance burdens on Alliance members. In addition to considering Regulations that address how businesses should handle CCPA requests received from consumers in the employee or B2B context, the Alliance also respectfully requests forbearance from enforcement of employee or B2B related violations to allow businesses to the necessary time to build and implement the necessary compliance policies and frameworks.

XIV. The Agency Should Delay Enforcement Until After Regulations Are Finalized

The Alliance recognizes that the Agency was given a tall order to meet the July 1, 2022 deadline and can understand the necessary but time-consuming steps it must take (and will continue to take) to draft and finalize these Regulations. The Alliance also recognizes the challenge with creating regulations that address privacy risk assessments, cybersecurity audits, and the use of automated decision-making.

That said, the Alliance asks the Agency to delay enforcement of these Regulations, given it has missed the July 1, 2022 deadline to adopt final regulations. News and media outlets subject to the CCPA need time to implement the Regulations once they are finalized. This will allow businesses, service providers, contractors, third parties, and in particular small publishers, the ability to take a reasonable amount of time to analyze and implement the Regulations. Alternatively, the Alliance respectfully requests that the Agency explicitly set out in the Regulations that the Agency shall not enforce against violations of the CPRA amendments if such violations occurred prior to July 1, 2023³⁴; or against violations with respect to obligations only found in proposed regulations; or, with respect to automated decision-making, privacy risk assessments, and cybersecurity audits, until six months after such obligations are addressed in finalized Regulations.

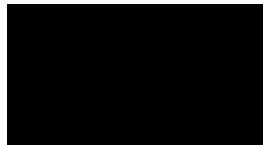
XV. Conclusion

It has never been more clear that a vibrant and thriving free press cannot be taken for granted. To that end, removing onerous business obligations and imposing restrictions that would inhibit the responsible use of digital advertising are critical to assuring that independent media does not cease to exist. Further, aligning privacy practices with consumer expectations can contribute to improving readers' trust in news at a time when it is under threat.

³⁴ Cal. Civ. Code §1798.185(d). "Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable."

The Alliance looks forward to working with the Agency to craft forward-thinking Regulations that balance consumer privacy with the needs of independent journalism (which is so critical to a functioning democracy), and that could serve as a model for other states and jurisdictions.

Sincerely,



Danielle Coffey
EVP & General Counsel
News Media Alliance

From: **Matt McGuire** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 14:58:40 (+02:00)
Attachments: Violet - CPPA Public Comment (Aug. 2022).pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find DeFi Labs GmbH aka Violet's comments on the proposed regulations.

Best,
Matt

--
Matt McGuire
General Counsel | Violet
[REDACTED]



August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Via Email (regulations@cpha.ca.gov)

RE: CPPA Public Comment

DeFi Labs GmbH (DeFi Labs) welcomes the opportunity to engage with the Agency on these critical privacy matters. We are a crypto-native company focused on building trust, transparency, and compliance through our highly customizable compliance and identity service, Violet. One of our core tenets, and that of the web3 community more broadly, is: “users own their data, not corporations.”¹ The Agency’s proposed regulations of private businesses are consistent with that tenet, and we support this important regulatory initiative.

The proposed regulations, however, are incomplete. Our core tenet is equally applicable to governments: “users own their data, not governments.” That protection is enshrined in many provisions of the United States and California Constitutions, but nothing in the Agency’s proposed regulations acknowledges that fact, despite being compelled by § 1798.185(a)(17) to issue regulations about the meaning of the “law enforcement agency-approved investigation” exception in § 1798.145.² California often leads the way on privacy protections in the United States, and it should do so here by clarifying when, how, and on what bases government actors can demand various categories of personal information from

¹ About, web3 Foundation (last visited Aug. 22, 2022), <https://web3.foundation/about/#:-:text=Web3%20Foundation%20believes%20in%20an,information%20and%20value%20are%20decentralized>.

² To be sure, the California Privacy Rights Act addresses “businesses,” but § 1798.145 is a critical provision when a business receives a law enforcement request and has to decide how to proceed. The Agency did not identify this issue as excluded in the Notice of Proposed Rulemaking. The Agency should take this opportunity to “further the purposes of this title” and ensure government actors are adequately justifying any requested intrusion into a person’s privacy by a third-party company or unwarranted retention of their data.



neutral third parties and under what circumstances third-party businesses can be forced to retain personal data for the sole reason of permitting future government access.

From “John Doe subpoena” fishing expeditions³ to requests for “voluntary” disclosure,⁴ government actors frequently target the data collected and stored by third-party businesses in privacy destroying ways that leave users with little practical recourse.⁵ Even more so than private businesses, government actors should operate transparently by willingly and publicly committing to similar data-access limitations to ensure peoples’ privacy isn’t unnecessarily compromised. We respectfully submit that the Agency should formally interpret “law enforcement agency-approved investigation” to require itself and other Californian government actors to be at least as protective of peoples’ privacy as private businesses.

About Violet

We created Violet, a highly customizable compliance and identity infrastructure for web3. Violet’s purpose is to provide a standardized method to issue compliance credentials and map smart-contract access controls on the Ethereum network *without forcing a user to disclose their identifying information to anyone else*. Violet achieves this purpose in a way intended to fulfill traditional

³ These are functionally indiscriminate subpoenas seeking evidence of illicit activity without particularized evidence, and when granted, compromise innocent peoples’ privacy rights on a quest to *maybe* identify bad actors. E.g., DOJ, IRS Target Tax-Evading Clients of Crypto Broker SFOX, Decrypt (Aug. 16, 2022), <https://decrypt.co/107578/doj-irs-tax-crypto-broker-sfox-john-doe>.

⁴ E.g., Testimony of Caitlin Chin, *Digital Dragnets: Examining the Government’s Access to Your Personal Data* (July 19, 2022), <https://www.csis.org/analysis/digital-dragnets-examining-governments-access-your-personal-data>; Angel Diaz, *When Police Surveillance Meets the ‘Internet of Things’*, Brennan Center for Justice (Dec. 16, 2020), <https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things>.

⁵ There are numerous examples of this, from the national security context that led to invalidation of the Privacy Shield in *Schrems II*, Case No. C-311/18, [2020] (Grand Ct.) (Ir.) at paras. 178-186, to the routine assertions in government cover letters that grand jury subpoenas should be kept confidential even in the absence of a statutory obligation to maintain secrecy or a neutral arbiter’s decision to issue a nondisclosure order for the matter.



compliance requirements like Know Your Customer (KYC), Know Your Business Customer (KYBC), sanctions checks, and anti-money laundering rules (AML) in an on-chain verifiable way that protects a user’s privacy. Violet’s operational flows and identity mechanisms tie into the larger, generalizable smart-contract framework and can be implemented to support any compliance regime that requires identity proofing.

Data protection and user privacy are foundational elements for Violet because, at the end of the day, a Violet credential is “humanbound” and thus very sensitive. Violet takes user sovereignty over their data seriously and *will never store personal information on-chain*. Access to personal information (or proofs relating to personal information) will always require user authorization. More specifically, the data Violet collects at registration – and that it relies on to verify ongoing user compliance with applicable legal requirements – is stored in an encrypted data vault where access requires a private key.⁶ Violet will launch with a self-service user portal intended to provide maximum transparency and control to anyone that opts to obtain a Violet credential.

To paraphrase an old adage: with great trust comes great responsibility. We are committed to protecting people’s privacy and living up to one of the central tenets of web3 – it’s your data, not ours.

Government Actors, like CPPA, Must Equally Respect User Privacy and Demonstrate that Commitment Through Binding Regulations

The Agency said it best in the text of proposed regulation § 7027: “The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer.” We completely agree, which is why Violet does not process or disclose any personal information, sensitive or otherwise, in ways other than (1) what a user agrees to upfront at registration, or (2) when a user seeks to use their Violet credential with a new smart contract that requires increased compliance checks. Protecting against disclosure of personal information without a person’s consent, opportunity to object, or opportunity to at least meaningfully understand why it is being disclosed is critical.

⁶ Violet is not yet available as a live product, although it will be live very soon along with a detailed privacy notice and transparent terms of service.



Although the Agency’s regulatory proposal is admirable in its focus on meaningfully protecting personal data from unwanted or unknown disclosure, the proposal fails to address one of the key sources responsible for unwanted or unknown data access: the government. Last month, for example, congressional testimony showed that “Apple, Google, Facebook (now Meta), and Microsoft together received approximately 125,000 U.S. legal requests for data from January to June 2021, involving 248,000 accounts.”⁷ To restate it: four, admittedly large, U.S.-based companies received *government requests for data involving more than a quarter million* accounts in the first half of 2021 alone. The graphs that accompany some of the transparency reports showing the number of requests received over time paint an even starker picture. And that’s just scratching the surface: the same congressional testimony also pointed out the incredible amount of personal data government agencies have been buying without a person’s knowledge or consent to that usage.⁸

These widespread, unjustified intrusions into personal privacy are absolutely troubling and inconsistent with the Agency’s proposed regulation. Avoiding unfettered and warrantless surveillance and data retention is central to why the web3 community broadly takes data protection and privacy so seriously. It’s not because there aren’t legitimate reasons for government access to data – the sad truth is there are bad actors, and under certain circumstances, governments do have the legal right to demand information about accounts that are linked to bad acts. It’s because the current practices being employed by many government actors and companies do not even come close to meeting the standards of transparency and minimization the Agency is pursuing in its proposed regulations. Government officials serve in a position of trust, have significantly greater power to infringe on a person’s liberty than a private actor, and should be held to a higher standard as a result. When it comes to data protection and privacy, no such higher standard exists or is being applied.

We encourage the Agency to revisit its proposal and specifically include provisions requiring transparency and a fulsome process before government

⁷ *Digital Dragnets*, *supra* note 4; *see also id.* n.3 (citing the transparency reports that provide even more granular detail on the depth of intrusion).

⁸ *See id.* & nn.6-9.



actors in California may demand information about a person from a third-party business. Options abound:

- prohibiting collection of personal data from third parties altogether absent a valid subpoena or similar compulsory process, including when asking businesses to retain data;
- limiting the type of personal data a government actor can access to what's absolutely necessary for an investigation (*e.g.*, no transaction history when the minimum information needed really is identification); and
- demonstrating in every case that the government actor tried and failed to obtain the required information directly from the user themselves before seeking it from a third-party business unless a court has signed off on a nondisclosure order.

Conclusion

Meaningful data protection and privacy safeguards are core tenets of Violet and the web3 community. We can have a safe, secure, and compliant web3 ecosystem that maximally preserves user privacy when that user is acting in good faith and that stops bad actors at the same time. We appreciate the Agency's efforts exhibited by the proposed regulations, but believe the Agency erred by not defining "law enforcement agency-approved investigation." The Agency should modify the proposed regulations and interpret that term to ensure personal information is properly protected from ongoing, unexpected, and vastly overbroad government intrusion.

Respectfully submitted,

Matthew R. McGuire
General Counsel | DeFi Labs GmbH aka Violet



From: **Leticia Garcia** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 19:06:25 (+02:00)
Attachments: August CGA CPRA Comments Final .pdf (4 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,

Attached are the comments from the California Grocers Association. Thank you.

Leticia Garcia
Director, State Government Relations
California Grocers Association

Cell [REDACTED]
Address 1005 12th Street Suite 200, Sacramento, CA 95814
Website www.cagrocers.com





August 23, 202

California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd., Sacramento, CA 95834

Dear Mr. Soublet,

On behalf of the members of the California Grocers Association (CGA), I write to provide feedback on the proposed updated language to the CPRA.

CGA is a non-profit, statewide trade association representing the food industry since 1898. CGA represents approximately 500 retail members operating over 6,000 food stores in California and Nevada, and approximately 300 grocery supplier companies. Traditional supermarkets in California employ more than 300,000 residents in virtually every community in the State.

Section 7002. Restrictions on the Collection and Use of Personal Information

With respect to how a business may use personal data that it collects, subsection (a) defines “reasonably necessary and proportionate” to mean “what an average consumer would expect when the personal information was collected.” This creates significant ambiguity since a business, consumer, and regulator may differ on what an average consumer expects. This also conflicts with the standard set forth in the statute—which is whether the collection is “reasonably necessary and proportionate to achieve the purposes” for which the personal data was collected or processed, not how an average consumer might expect the data to be used.

Below is suggested amendments this section.

7002(a): A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ the context in which the personal information was collected. A business shall obtain the consumer’s explicit consent in accordance with section 7004 before collecting,

using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.

Section 7012. Notice of Collection

CGA requests clarification regarding personal information when it is collected offline. Our grocery retailers often collect personal information over the phone to pay for an order, such as a cake or catering order. The personal information being collected includes, but is not limited to, name, credit card information, billing zip code, and phone number.

Section (d) prohibits a business from collecting personal information from the consumer if the notice of collection is not given at the time of collection. This will cause problems for our members and their interaction with customers.

Employees may not be aware they need to provide the notice every instance they take a form of payment over the phone, even though their information will only be processed for payment.

Section (d) also causes confusion because it can be interpreted to conflict with the example in subsection (c)(5) where it states a business "may" provide the notice orally if personal information is being collected over the phone.

CGA requests the agency to make these clarifications in regards to offline personal information collection.

Section 7025. Opt-Out Preference Signals

While we applaud the efforts to do a universal opt-out preference for consumers, current draft language leaves room for improvement and clarification.

The requirements to honor universal opt-out methods should not go above and beyond than the capabilities of eligible universal opt-out methods that are available in the marketplace.

Just as businesses are required to process opt-out preferences, there should be ability for the consumer to turn off the opt-out function and have it apply across board. As currently drafted, the regulations deprive the consumer of the ability to fully control opt-out preferences.

Section (b) should be amended as follows:

A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

- (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

~~(2)~~(3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

One last request for this section is that it not conflict with the CPRA statute, which gives businesses the option to honor universal opt-out methods as opposed to making it a requirement.

Section 7026. Conveying Opt-Out Preferences to Third Parties

Subsection (f) has some compliance issues that can arise from our grocery retail members. Once again we would like to highlight our single store operators and independent operators. This section of our membership generally contracts with third parties and does not have the capability to contact the third party provider partners that interact with the consumers data.

We suggest amending subsection (f) to be limited only to the third parties the business has sold or shared the consumer's personal data and include the disproportionate effort standard.

CGA would like to emphasize the inclusion of the disproportionate effort standard. CGA membership, especially single store and independent operators, do not have the bandwidth or resources to follow the chain of data selling or sharing through third party operators. This would require for them to hire one or a team of data privacy experts or contract with a third party. This could be very costly for an industry that survives on razor thin margins.

Below is the suggested language to amend the following subsection:

7026(f)(3): Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information ~~available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises,~~ that the consumer has made a request to opt-out of sale/sharing and directing them ~~to~~ to comply with the consumer's request unless such notification proves impossible or involves disproportionate effort and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period. In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.

CGA appreciates the opportunity to comment to the proposed language. We look

forward to working with you on the implementation of these rules.

Si



Leticia Garcia
Director, State Government Affairs
California Grocers Association

From: **Chris Pedigo** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comments
Date: 23.08.2022 19:15:11 (+02:00)
Attachments: DCN-Comments-re-CPRA-Regulations 082322.pdf (4 pages), DCN-Preference-Signal-Analysis.pdf (4 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon – please find comments from Digital Content Next related to the proposed regulations for the California Privacy Rights Act as well as an analysis of the role of opt out preference signals in the CPRA. If you have any questions, please feel free to contact me directly.

Sincerely,

Chris Pedigo
SVP, Government Affairs
Digital Content Next
[REDACTED]



August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd., Sacramento, CA 95834

RE: CCPA Public Comment

To Whom It May Concern,

We appreciate the opportunity to comment on the draft regulations to implement the California Privacy Rights Act (CPRA). Digital Content Next (DCN), representing many of the Internet's most trusted and respected publishing brands, appreciates the opportunity to submit comments in the above-captioned proceeding. Founded in 2001, DCN is the only trade organization dedicated to serving the unique and diverse needs of high-quality digital content companies that manage trusted, direct relationships with consumers and marketers.¹ DCN's members are some of the most trusted and well-respected media brands that, together, have an unduplicated audience of 223,098 million unique visitors or 100 percent reach of the U.S. online population.

Methods for Requests to Delete, Correct or Know

We appreciate that the draft regulations allow for businesses that operate exclusively online to provide only an email address for consumers to exercise their rights to delete, correct or know information that the business holds about them. Coupled with the requirement that the business must also consider how they primarily interact with consumers, we believe the regulations provide sufficient flexibility to comply with the law while providing a quality consumer experience. However, there is significantly less flexibility for businesses that do not operate "exclusively online." For these businesses, they must offer a toll-free number and a web form to consumers. We are concerned that requiring these businesses to offer a toll-free number would be unduly burdensome and may not match with how a consumer interacts with the company. We recommend that Section 7020 (a) be amended (new text in italics) to apply to a "business that operates *primarily* online and has a direct relationship with a consumer."

¹ See <https://digitalcontentnext.org/membership/members/> for a listing of our current members.

Opt Out Signals

We are pleased that the CPRA and your draft regulations explicitly allow for consumers to use an opt-out preference signal. DCN has been supportive in the development of the Global Privacy Control (GPC), as one potential mechanism, to facilitate users being able to clearly express their privacy preferences. This is especially important as it facilitates being able to communicate to companies with which they are not choosing to interact in a certain context.

We agree that these signals should not require a user to take specific action to confirm or authenticate the signal. Their purpose is to eliminate consumer friction and most rapidly align with the consumer's expectations without requiring additional data to be supplied or effort to be taken. These opt-out signals may be turned on by default as written in the law especially to the extent that the signal is clearly marketed to the consumer as a privacy-enhancing tool. We are concerned that attempts to require authentication of consumers might simply be an attempt to avoid having to honor a consumer's preference to stop the sharing or sale of data. In 2021, we received analysis² from our outside counsel which advised that opt-out preference signals, such as the GPC, are valid under the CPRA and that businesses are not permitted to routinely verify or authenticate opt-out preference signals.

In addition, we applaud the inclusion of Section 7026 "Requests to Opt Out" (f) (3) and Section 7052 "Third Parties." Both of these sections outline how third parties must revert to the role of service providers when they receive a consumer's opt out signal from the publisher. Given the large number and varied types of third parties involved in the creation, delivery and monetization of digital products and services, it is imperative that there are clear rules for the road when a consumer expresses a preference to opt out of the sale or sharing of data. We appreciate Section 7026 (f)(3) and Section 7052 because they help ensure that third party partners clearly understand their obligations while not placing the burden on publishers for compliance by the entire ecosystem.

However, we have concerns about some of the requirements in the proposed regulations.

First, we are concerned about the requirement that businesses display in real time whether they have processed a consumer's opt-out preference signal. In addition to the significant burden on technical and employee resources to implement this functionality, we are concerned that the consumer's screen, especially on smaller devices, may become overly crowded with disclosures and links as required under California law. Further, it does not appear that the text of the CPRA supports this requirement. Since businesses are required to disclose how they comply with the CPRA in their privacy policies, we believe it is best not to require a real-time disclosure at this time.

Second, Section 7025 (c)(7) "Illustrative Examples" envisions a scenario (B) where a logged-in consumer visits a business' website via a browser with an enabled opt-out preference signal. In the example, it is suggested that the business should apply the opt-out preference to the business'

² https://digitalcontentnext.org/wp-content/uploads/2022/08/DCN-Preference-Signal-Article119773980_1.pdf

entire relationship with the consumer including to offline sales or sharing. In this scenario, we are concerned that it may be inappropriate to extend that opt-out preference to the entirety of the business' relationship with the consumer. From a technical perspective, it may be very difficult for publishers to identify the consumer in other contexts. For example, a consumer may only be logged in with an email address and the publisher may not know that the consumer is subscribing to a print edition under a real name and address. Extending the opt out request across the entire relationship may be too complicated and may inadvertently require companies to collect more data about consumers just in case they decide to opt out. In addition, the consumer has different expectations in different contexts regarding the use of her data. Consumers generally expect first parties to collect and use data about them to enhance their experience on the site or app, ensure proper functionality and tailor advertising based on previous visits. In this trusted, first party relationship, the consumer is more aware of the data collection and can object to the first party either by communicating directly with the company or by choosing not to visit the company's site or app again. For example, she may enable the opt-out preference signal on her mobile device's browser because she is concerned about unknown third parties collecting location data. But, she may have no intention of impacting data collection on other devices like a television or even in a physical store where unknown third parties are less prevalent. Indeed, she may expect the first party to remember past interactions with the site or app to help improve her experience and enhance her relationship with the first party.

Third, we are concerned about Section 7026 (a)(4) which states that having a cookie notification or tool is not sufficient to provide an opt out of sharing. We agree that a consumer's opt out means the business must not sell or share that consumer's data. However, in some cases, cookies can be a reliable tool to store a consumer's preference and ensure that third parties can honor the consumer's preference. We are concerned that Section 7026 (a)(4) may cause confusion about the use of cookies to communicate a consumer's opt out preference.

Finally, publishers are concerned that browser or device companies may seek to promote their own preference signals to unfairly favor their own business. As such, we urge you to carefully monitor how the dominant browser and device companies honor these opt out signals as well as any attempts to develop their own preference signals.

Employee and Business-to-Business Data

The California Legislature carved out employee data and business-to-business data from the definition of personal data. However, that carve-out is set to expire at the beginning of 2023. We are concerned that the draft regulations provide no guidance for companies on how to comply with the law regarding employee data and business-to-business data. It might be helpful to publicly lay out a plan for when the agency will provide guidance so that companies can be prepared to act.

We appreciate the opportunity to offer these comments for your review and look forward to working with you to protect the privacy of California consumers.

Sincerely,



Chris Pedigo
SVP, Government Affairs
Digital Content Next

MEMORANDUM

To: Digital Content Next

From: Todd D. Daubert
William M. Krouse

Date: November 8, 2021

Subject: **CPRA Right to Opt Out - Unpacking Preference Signals**

Less than a year after the California Consumer Privacy Act (“CCPA”) went into effect, Californians voted in favor of even more privacy rights and protections for consumers by passing Proposition 24 so that the California Privacy Rights Act (“CPRA”) would become law. The CPRA expands the data privacy obligations of businesses to address perceived shortcomings of the CCPA by making it easier for consumers to exercise their rights and protect their privacy. As the architect of the CPRA, Alastair Mactaggart, has explained, the “playing field is not remotely level, because you have the smartest minds on the planet trying to make that as difficult as possible for you.”¹ The focus of the CPRA is to level the playing field.

One goal of the CPRA is to ensure that each business fully discloses how it collects and uses personal information and to give consumers more ways to control their personal information. For example, the CPRA expands the opt-out right of consumers to cover not only the sale of their personal information, but also the sharing of their personal information for cross-context behavioral advertising, even when there has been no sale.² This expansion requires businesses to be more transparent about when and why they transfer personal information to others, and to honor requests from consumers that their personal information not be sold to others or transferred for the purpose of facilitating cross-context behavioral marketing.

Another goal of the CPRA is to make it easier for consumers to exercise their privacy rights. Under the CPRA, consumers can exercise their privacy rights by engaging directly with businesses or by

¹ Tom Simonite, Lawmakers Take Aim at Insidious Digital ‘Dark Patterns’, *Wired*, Jan. 29, 2021, available at: <https://www.wired.com/story/lawmakers-take-aim-insidious-digital-dark-patterns/>.

² The term “cross-context behavioral advertising” is defined as “the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.” Cal. Civ. Code § 1798.140(k).

relying on technologies like preferences signals or authorized agents they have designated to act on their behalf.³

Opt-out preference signals play an important role in lowering the burdens that consumers face when exercising their privacy rights under the CPRA, particularly for consumers who choose to rely on authorized agents.⁴ If businesses did not have to honor opt-out preference signals, authorized agents would have to engage directly with each individual business on behalf of consumers rather than rely on a global opt-out preference signal and engage directly on an exceptions basis only with businesses for which the consumer does not wish to opt out (or consumers could do so themselves when engaging with preferred businesses). The CPRA facilitates efficiency by requiring businesses to honor opt-out preference signals sent by authorized agents.⁵ By contrast, the CPRA does not require businesses to honor opt-out preference signals sent directly by consumers, presumably because it is easier for consumers to express their preferences when engaging directly with businesses. However, if a business declines to honor opt-out preference signals sent directly by consumers, it must instead provide clear and conspicuous “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on their homepages or provide a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal information and to limit the use or disclosure of their sensitive personal information.⁶

³ The term “authorized agent” is defined as “a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.” 11 CCR § 999.301(c).

⁴ The CPRA expands on the current treatment of preference signals in the California Attorney General’s regulations to implement the CCPA. *See* 11 CCR § 999.315(c) (“If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to [opt out] of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.”); Cal. Civ. Code § 1798.135(c) (“A consumer may authorize another person solely to [opt out] of the sale of the consumer’s personal information on the consumer’s behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, *pursuant to regulations adopted by the Attorney General.*”) (emphasis added). Although the CPRA does not define the term “opt-out preference signal”, opt-out preference signals are one type of “user-enabled global privacy control,” which the CCPA regulations define as “a browser plug-in or privacy setting, device setting, or other mechanism” that communicates or signals the consumer’s choice to opt out. 11 CCR § 999.315(c).

⁵ *See* Cal. Civ. Code § 1798.135(e). The implementing regulations will provide more detail on how businesses must recognize and honor opt-out preference signals. *See* Cal. Civ. Code § 1798.185(a)(20).

⁶ *See* Cal. Civ. Code § 1798.135(b)(1) (“A business shall not be required to [provide clear and conspicuous “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on their homepages or provide a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal information and to limit the use or disclosure of their sensitive personal information] if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal...”); *see also* Cal. Civ. Code § 1798.135(b)(3) (“A business that complies with [providing clear and conspicuous “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on their homepages or providing a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal information and to limit the use or disclosure of their sensitive personal information] is not required to [honor opt-out preference signals received directly from consumers]. For the purposes of clarity, a business may elect whether to comply with [providing clear and conspicuous “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on their homepages or providing a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal

The CPRA makes clear that businesses must always accept opt-out preference signals sent by authorized agents, even if they choose not to honor opt-out preference signals sent directly by consumers:

[A] business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General, regardless of whether the business has elected to [provide clear and conspicuous “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on their homepages or provide a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal information and to limit the use or disclosure of their sensitive personal information] or [honor opt-out preference signals received directly from consumers].⁷

In light of this obligation, businesses that sell or share information under the CPRA must, at a minimum, recognize opt-out preference signals sent by authorized agents on behalf of consumers and, upon recognition, no longer sell or share the personal information of the consumer on whose behalf the signal was sent, as well as limit the use of the consumer’s sensitive personal information.⁸

The CPRA’s endorsement of opt-out preference signals extends far beyond requiring businesses to honor opt-out preference signals sent by authorized agents. For example, businesses are not permitted to routinely verify opt-out preference signals by, for example, seeking to confirm that the signal was sent with the individual’s consent. This is in sharp contrast with the requirement that businesses verify all other privacy rights requests before honoring them.⁹ Specifically, a business can only seek to verify an opt-out preference signal if it has a “good faith, reasonable, and documented belief” that the signal is fraudulent or sent without the individual’s consent.¹⁰ To have this reasonable belief, a business would need prior documentation that opt-out preference signals received from a particular sender or opt-out preference tool, or signals sent on behalf of a particular consumer, are likely fraudulent. Even with this documentation, a business can only request additional information from the consumer or authorized agent to verify whether the opt-out preference signal is valid, and then reject the signal only if the signal cannot be verified as valid. Although the CPRA states that opt-out preference signals require the sender’s consent, it does not address the type or form of consent required or how consent may, or must, be documented.¹¹ However, the type of consent necessary to send an opt-out preference signal is ultimately not for the business receiving the signal to consider since businesses are not routinely permitted to authenticate opt-out signals. The CPRA also supports opt-out preference signals by explicitly prohibiting businesses from responding to opt-out preference signals in a manner that would interrupt or degrade the

information and to limit the use or disclosure of their sensitive personal information] or [honoring opt-out preference signals received directly from consumers].”).

⁷ See Cal. Civ. Code § 1798.135(e).

⁸ *Id.*

⁹ See Cal. Civ. Code § 1798.135(c)(1); see also 11 CCR § 999.315(g) (“A request to [opt out] need not be a verifiable consumer request.”).

¹⁰ 11 CCR § 999.315(g).

¹¹ See Cal. Civ. Code § 1798.135(b)(1).

functionality of the consumer's browsing experience, including by displaying a notification or pop-up.¹² The CPRA's support goes as far as requiring that opt-out preference signals be simple to setup and use for consumers. For example, an opt-out preference signal's setup page may only provide up to three opt-out choices: (a) "Do Not Sell or Share My Personal Information"; (b) "Limit the Use of My Sensitive Personal Information"; or (c) a global opt-out for both.¹³

As a practical matter, businesses may find it difficult, if not impossible, to distinguish between opt-out preference signals sent by persons authorized by consumers to act on their behalf, which businesses must honor, and opt-out preference signals sent directly by consumers, which businesses are not required to honor if they instead provide clear and conspicuous "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links on their homepages or provide a single, clearly labeled link on their homepages that allows consumers to opt out of the sale or sharing of their personal information and to limit the use or disclosure of their sensitive personal information. If a business is unable to distinguish between opt-out preference signals from authorized agents and opt-out preference signals from consumers, the business can simply honor all opt-out preference signals that it receives, in which case the business would not be required to provide any "Do Not Sell or Share My Personal Information" or "Limit the Use of My Sensitive Personal Information" links on their homepages.

We expect that the implementing regulations for the CPRA and the new California Privacy Protection Agency ("CPPA") will provide additional clarity about how businesses can meet their obligations to honor opt-out preference signals, and we are confident that the CPPA's guidance will provide additional reasons why businesses should honor opt-out preference signals. No matter what the CPPA or implementing regulations require, the spirit of the CPRA, which reflects the expectations of California consumers, favors transparency and trust, not obfuscation and obstacles. Businesses that earn the trust of consumers are far more likely to form strong bonds with consumers and be permitted by consumers to meaningfully engage with their personal information. Trust starts with honoring both the privacy preferences of consumers and the means by which the consumers prefer to communicate.

¹² See Cal. Civ. Code § 1798.185(a)(20)(B)(v).

¹³ See Cal. Civ. Code § 1798.185(a)(19)(A)(vi).

From: **Hilary Cain** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment - Alliance for Automotive Innovation
Date: 23.08.2022 19:45:57 (+02:00)
Attachments: Auto Innovators Comments CPPA NPRM FINAL 8.23.22.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good Afternoon –

Please find attached comments from the Alliance for Automotive Innovation in response to the Notice of Proposed Rulemaking.

Cheers,
Hilary

Hilary M. Cain

Vice President - Technology, Innovation, & Mobility Policy

O: [REDACTED]

Alliance for Automotive Innovation

1050 K Street, NW - Suite 650 Washington, DC 20001

autosinnovate.org - [twitter](#) - [linkedin](#)





August 23, 2022

Mr. Brian Soublet
California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

RE: California Consumer Privacy Act Regulations Notice of Proposed Rulemaking

Dear Mr. Soublet:

The Alliance for Automotive Innovation (“Auto Innovators”) welcomes the opportunity to provide feedback to the California Privacy Protection Agency (“Agency”) on its Notice of Proposed Rulemaking (“NPRM”) on *California Consumer Privacy Act* (“CCPA”) regulations. We certainly share your goals of protecting consumer privacy and look forward to continued engagement and collaboration with you on this important issue.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 98 percent of cars and light trucks sold in the United States. In addition to motor vehicle manufacturers, members of Auto Innovators include original equipment suppliers, technology companies, and others within the automotive ecosystem. The auto industry is the nation’s largest manufacturing sector, contributing \$1.1 trillion to the United States economy. As a significant engine for our nation’s economy, the auto sector is responsible for 10.3 million jobs and \$650 billion in paychecks annually.

The auto industry is committed to protecting consumer privacy. In fact, in 2014, the auto industry came together to develop the *Privacy Principles for Vehicle Technologies and Services*. The Principles, which are enforceable by the Federal Trade Commission, represent a proactive and unified commitment by automakers to protect identifiable information collected through in-vehicle technologies.

Our comments below build on our comments to the Agency in response to its invitation for preliminary comments on proposed rulemaking and at the May 4 pre-rulemaking stakeholder session. They are primarily focused on areas within the proposed regulations that may have inadvertent or unintended impact on the auto industry and its ability to deliver a cleaner, safer, and smarter transportation future. We welcome the opportunity to discuss these issues with you directly and to work together collaboratively to address them.

Effective Date

Auto Innovators previously requested that at least 12 months be provided between the finalization of this important and consequential rulemaking and the effective date of any new obligations or requirements. We noted that our member companies take their compliance obligations seriously and need adequate time to align their processes and mechanisms with any new regulatory requirements. We respectfully reiterate this request for sufficient lead time.

Moreover, any new obligations in the regulations should be prospective and apply only to data collected after the regulation's effective date. For example, the Agency should reconsider the provision within § 7014 of the proposed regulations that requires a business to obtain the consent of the consumer before using or disclosing sensitive personal information the business collected "during the time the business did not have a notice of right to limit posted." This appears to create an obligation with respect to data collected before the regulations and the requirement to post a "notice of right to limit" takes effect.

Providing Notice

For purposes of providing notice to opt-out of sale/sharing, § 7013 of the proposed regulations requires a business that sells or shares personal information that it collects through a connected device to provide notice "in a manner that ensures that the consumer will encounter the notice while using the device." Section 7014 similarly requires that a notice to limit the use of sensitive personal information be provided "in a manner that ensures that the consumer will encounter the notice while using the device" if the business uses or discloses sensitive personal information that it collects through a connected device.

Many auto companies do not currently have the capability of providing these sorts of consumer notices in the vehicle. In these cases, the ability to provide such in-vehicle notices will almost certainly require vehicle engineering changes that may take years to integrate into production vehicles. To address this, we urge the Agency to provide some flexibility by allowing these notices to be provided in other manners that are regularly used by consumers in connection with the connected device.

If the Agency maintains a requirement that a business provide notice in a manner that ensures that the consumer will encounter it while using the device, we request that the Agency exempt vehicles that are already in the market or have already been produced if such vehicles do not have that capability. We further request that the Agency provide sufficient lead-time (i.e., at least three years) for auto companies to develop and integrate this capability into new vehicles.

In addition, § 7013 and § 7014 indicate that, if a business provides consumers with the opportunity to exercise their right to opt-out of sale/sharing through a "Do Not Sell or Share My Personal Information" link or their right to limit through a "Limit the Use of My Sensitive Personal Information" link, the links must "immediately effectuate the consumer's right" and "have the immediate effect" of opting the consumer out of the sale or sharing or personal information or limiting the use and disclosure of the consumer's sensitive personal information. However, § 7026 and § 7027 provide businesses up to 15 business days from the date the business receives a consumer's request to cease the selling or sharing of the consumer personal information or to limit the use and disclosure of the consumer's sensitive personal information. To ensure that businesses have sufficient time to responsibly process a request to opt-out of selling/sharing or a request to limit, we urge the Agency to clarify that the business must immediately register the consumer's request following the use of "Do Not Sell or Share My Personal Information" link

or a “Limit the Use of My Sensitive Personal Information” link, but not necessarily process that request immediately. To achieve this, we suggest that the language of § 7013 be modified to read “immediately effectuate the consumer’s right to opt-out of sale/sharing in accordance with subsection 7026(f)” and that the language of § 7014 be modified to read “immediately effectuate the consumer’s right to limit in accordance with subsection 7027(g)”.

Right to Know

We appreciate changes that were made to the right to know, including language that clarifies that a business should verify a consumer making such a request. This important change appears to address some of our concerns about auto companies having to disclose sensitive vehicle information, such as vehicle location information, to consumers who may not have been using the vehicle when the sensitive vehicle information was generated.

We have previously noted that much of the data that is generated and collected from vehicles is from onboard computer systems and sensors and relates to the operation and functioning of the vehicle and its systems. This data is very technical in nature and of little use to the average consumer. In addition, this information frequently contains detailed data elements related to each vehicle system and component over the life of the vehicle. Since the average life of a vehicle is nearly 12 years, the volume of the data that may be responsive to a request for specific pieces of information would be vast and likely overwhelming for the consumer.

Section 7024 of the proposed regulations allows a business to deny a consumer request for access to personal information if it involves a “disproportionate effort.” We have previously requested that the Agency deem disclosure of operational data for a device owned or used by a consumer beyond the preceding 12 months as involving a disproportionate effort. While we appreciate that the Agency has provided a definition of “disproportionate effort” in the proposed regulations, the definition does not yet provide the auto industry with the clarity that it is seeking with respect to this issue. For this reason, we respectfully reiterate our request for clarity on this specific point.

Right to Correct

We appreciate modifications that were made to the proposed regulations related to the ability of a business to deny a consumer’s request to correct if it determines that the contested information is more likely than not accurate based on the totality of circumstances, including the documentation relating to the accuracy of the information. These changes seemingly address some of our concerns about requests that auto companies may receive to correct data generated by vehicle systems and components, including sensors.

In our prior comments, we recommended that the Agency clarify that a business is not required to correct information that it has received from a third party. In these cases, we recommended that the business be permitted to refer the consumer to the third party from which it received the personal information for correction. However, in cases where the business is not the source of the information that the consumer contends is inaccurate, § 7023 of the proposed regulations unnecessarily increases the burden on a business by requiring a business to not only process the consumer’s request to correct, but to also provide the consumer with the name of the source from which the business received the alleged

inaccurate information. We reiterate our request that, when the business is not the source of the information, the business be permitted to refer the consumer to the source of the information for correction.

Moreover, the proposed regulations also require a business to note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. Under the proposed regulations, this requirement does not apply to requests that are determined to be fraudulent or abusive. We suggest that requests that are denied based on “inadequacy in the required documentation” also be exempted from this requirement. With this change, the requirement to note that the accuracy has been challenged would remain for circumstances where the request was denied based on a conflict with federal or state law or on the contention that compliance proves impossible or involves a disproportionate effort.

Finally, the proposed regulations include a new provision that requires a business, upon request, to disclose all of the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer’s request to correct. The new provision further specifies that disclosure under this provision is not considered a response to a request to know which is limited to two requests within a 12-month period. The requirements of this section are seemingly broader than is required to achieve its goals. If the goal is to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer’s request to correct, it should be sufficient for the business to disclose to the consumer only the specific pieces of personal information that were subject to the consumer’s request to correct. We suggest that the proposed regulations be modified along those lines.

Consumer Verification for Request to Opt-Out and Request to Limit

Section 7060 of the proposed regulations clarify that a business cannot require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. We recommend that the Agency create an exception to this language where the sharing of personal information or the use of sensitive personal information is necessary to support a product or service previously requested by the consumer. For example, if the consumer has previously opted into a service through which vehicle data is shared with an insurance company or a service in which geolocation information may be collected following a collision to dispatch emergency responders to the scene of the incident and opting out of sharing or limiting the use of sensitive information would essentially void the ability of the consumer to continue to receive those requested services, it would be entirely appropriate for the business to verify that the consumer is in fact who they claim to be. This would help avoid a situation where someone other than the person who opted into those services could void those services without the person’s knowledge or consent.

Contract Requirements for Third Parties

Section 7053 of the proposed regulations require extensive new contract requirements with third parties with which a business sells or shares a consumer’s personal information. Since the development of new contracts or the renegotiation of existing contracts with third parties may take considerable time, we respectfully request sufficient time (i.e., no less than 6 months) to develop or renegotiate contracts consistent with these new requirements.

Agency Audits

Section 7304 of the proposed regulations permit the Agency to audit a business “if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security.” We recommend that this basis for an audit be removed. The Agency should not have the right to audit a company for this reason alone without any other indication that there has been a possible violation of the CCPA or in the absence of a history of noncompliance with the CCPA or any other privacy protection law.

We further recommend that a reasonable statute of limitations (e.g., three years) be established with respect to the Agency’s ability to audit a business. In other words, the Agency’s ability to audit compliance should not be limitless and should instead be confined to a specified number of years prior to the initiation of the audit.

Consumer privacy remains critically important to the auto industry. We appreciate the opportunity to provide this feedback on the NPRM and look forward to continuing to work with the Agency on this and other privacy-related matters.

Sincerely,

A large black rectangular redaction box covering the signature area.

Hilary M. Cain
Vice President
Technology, Innovation, & Mobility Policy

From: **privacyprosh** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 20:06:18 (+02:00)
Attachments: CPPA Public Comment.pdf (9 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

CPPA Public Comment attached. Thank you.

Sent with [Proton Mail](#) secure email.

August 23, 2022
California Privacy Protection Agency
Attn: Brian Soublet
Submitted via e-mail to regulations@coppa.ca.gov
CPPA Public Comment

We respond below to the California Privacy Protection Agency's ("**CPPA**" or "**Agency**") [Notice of Proposed Rulemaking](#) by submitting written comments on the proposed regulatory action, specifically to propose certain modifications to the Text of Proposed Regulations ("**Regulations**") that will implement the California Privacy Rights Act of 2020 (the "**CPRA**"). As the authorized representatives of a multinational e-commerce and online advertising company with a mid-sized California operation, including several hundred California employees, we appreciate the opportunity to submit relevant comments for the Agency's consideration on behalf of this interested party.

INTRODUCTION

Our comments focus on only a few main provisions in the Regulations that warrant revision, so that the final Regulations will meet the OAL's substantive review standards (Authority, Reference, Consistency, Clarity, Nonduplication, and Necessity. Cal. Gov. Code §11349-11349.6), and satisfy the Agency's mandate to implement regulations that are necessary to effectuate the CPRA, provide added clarity to the interpretation of the statute, are consistent with the provisions of the statute and other regulations, do not exceed the Agency's rulemaking authority, and are feasible for affected parties to implement in a timely and cost-effective manner in order to effectively protect California consumers' privacy rights.

Our suggested revisions and redlines to the Regulations are set forth at the end of

each Section.

A. PROPOSED REGULATIONS SECTION 7025: OPT-OUT PREFERENCE SIGNALS

1. Summary of Comment

The plain text of the CPRA statute (§1798.135) allows businesses to choose between publishing links to enable consumers to opt out or honoring opt-out preference signals for this purpose. The draft regulations (§7025) eliminate the statutorily-provided choice by requiring a business to recognize and process opt-out preference signals from consumers even if the business provides the labelled opt-out links. As the draft Regulations contradict the express language of the statute, we suggest that the Regulations be modified to align with the actual text of CPRA, which does not warrant nor support the Agency's interpretation that no choice between the methods was intended. In addition, the proposed Regulations fail to meet the Agency's mandate in §1798.185(a)(19) to provide sufficient and clear regulations regarding the technical specifications of an opt-out preference signal to be sent via platform, technology, or mechanism.

In particular, the provisions of §7025 of the proposed Regulations do not satisfy the consistency, clarity, or necessity standards under the APA for OAL review and approval. (Cal Gov. Code §11349(d) (defining "**consistency**" as "being in harmony with, and not in conflict with or contradictory to, existing statutes, court decisions, or other provisions of law," "**clarity**" as being "written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them," and "**necessity**" as when "the record of the rulemaking proceeding demonstrates by substantial evidence the

need for a regulation to effectuate the purpose of the statute ... that the regulation implements, interprets, or makes specific, taking into account the totality of the record”).

2. Substantive Reasoning for Recommended Revisions

a. Consistency

Section 1798.135(a)-(b) of the CPRA sets forth two methods that businesses can implement to enable consumers to limit the sale and sharing of their personal information, and/or limit the use and disclosure of their sensitive personal information. Subdivision (a) of §1798.135 describes the publication and implementation of labelled links that allow consumers to opt out (either (i) a link to enable opt-out of sale/sharing and (ii) a link to limit use of sensitive personal information, or (iii) a single link to accomplish both), while subdivision (b) lays out a method of recognizing opt-out preference signals “sent with the consumer’s consent by a platform, technology, or mechanism”

The text of section 1798.135 specifies in three places that a choice or option between these two methods on the part of the business is intended by the statute. First, subdivision (b)(1) of §1798.135 states as follows: “A business shall not be required to comply with subdivision (a) if the business allows consumers to opt-out . . . through an opt-out preference signal” Second, the statute also clearly provides the converse in the first sentence of subdivision (b)(3): “A business that complies with subdivision (a) [link method] is not required to comply with subdivision (b) [opt-out preference signal method].” Third, in case the above two statements did not make clear that an option to be elected by the business was intended, the second sentence of subdivision (b)(3)

expressly re-iterates the choice for clarity: “For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b). (emphasis added).

The draft Regulations in section 7025 are inconsistent with the CPRA because they remove a business’s option to elect the opt-out method to implement which is clearly provided in the statute. Despite the statute’s language in §1798(b)(3) that “a business may elect whether to comply with subdivision (a) or subdivision (b),” the draft regulations state:

“[Civil Code Section 1798.135] does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner.” §7025(e).

The Initial Statement of Reasons (ISOR) submitted with the draft Regulations as part of the rulemaking proceeding record further clarifies the meaning and intent of draft regulation section 7025(e) to remove the option to elect an opt-out method:

“[T]hese regulations make clear that businesses must comply with an opt-out preference signal regardless of whether or not they post the identified opt-out links.” ISOR at 38.

The draft Regulations’ blatant contradiction of the CPRA’s plain language and clear intent to offer businesses an option cannot meet the consistency standard for the OAL’s substantive review.

b. Clarity

The provisions of §7025 of the proposed Regulations do not meet the “clarity” standard. Rather than “issuing regulations that define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology or mechanism” and meeting the six specified criteria mandated of the Agency in section

1798.185(a)(19)(A), the draft Regulations invent and define an unnecessary concept of “frictionless” processing of opt-out preference signals in order to justify the Agency’s position on opt-out choice. This concept is neither supported by the CPRA statute nor sufficiently specified, from a technical standpoint, to enable consumers to send and businesses to receive, opt-out preference signals that clearly communicate consumer choice and also enable a consumer to change their communicated preference using the same method.

The provisions of draft Regulation §7025 fail the “clarity” standard and thus do not represent the most effective and least burdensome way to effectuate the consumer right to opt-out.

c. Necessity

Finally, the provisions of Section 7025 do not meet the “necessity” standard and exceed the rulemaking authority of the Agency. Removing the ability of businesses to choose which opt-out method to implement is unnecessary to effectuate the purposes of the CPRA regarding a consumer’s right to opt-out: to ensure that a consumer will have at least one option to effectuate an opt-out right. Businesses that either provide a link to a mechanism that allows consumers to opt out or honor opt-out preference signals, each effectuate the purpose of CPRA section 1798.135(a)-(b) according to the statute.

Although the ISOR states that section 7025(e) is “necessary to respond to incorrect interpretations in the marketplace that complying with an opt-out preference is optional for the business,” (ISOR at page 37), the reference to “necessity” in this context demonstrates a mischaracterization of the evaluation standard, because the Agency’s interpretation is not supported by the plain language of the statute nor needed to ensure

the plain meaning is effectuated. Instead, the provisions of Section 7025 of the proposed Regulations represent unauthorized lawmaking that changes the plain meaning of the statute, rather than rulemaking to elucidate the public understanding of unclear statutory text.

3. Recommended Revisions to Regulations Section 7025

We urge that the top priority of the Regulations regarding opt-out preference signals should be to provide businesses with more guidance with respect to technical specifications. We propose that the draft Regulations require the CPPA to recognize an opt-out preference signal technology or specification. The draft regulations fail to set a standard for opt-out preference signals, but the CPPA could still provide clarity by formally recognizing specific acceptable technology/ies or process(es).

Finally, with respect to the text of section 7025(e), strike all the text before the sentence “If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.” *Id.* The section as written is too patently inconsistent to successfully pass the substantive review by OAL under the APA. It is also unclear and unnecessary to provide the most effective and least burdensome effectuation of the CPRA.

B. PROPOSED REGULATIONS SECTION 7023: REQUESTS TO CORRECT

1. Summary of Comment:

Section 7023's requirement that a business provide the source of the information when a consumer requests correction of inaccurate information held by the business, but for which the business is not the source, is unnecessary to effectuate the purpose of

the CPRA, is inconsistent with other provisions of the statute, and is not the most effective and least burdensome way to effectuate the purpose of the consumer's right to correction. This requirement should be eliminated or limited to only apply in certain circumstances where the business is otherwise unable to effectively maintain the correction of the information in its own records because of the manner in which it is communicated from another source.

2. Substantive Reasoning for Recommended Revisions

a. Consistency

The requirement for businesses to disclose specific sources of personal information in a response to requests to correct inaccurate personal information is inconsistent with the CPRA because it expands both the right to correct and the right to know beyond what the statute provides.

Section 7023(i) of the draft Regulations states:

“Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.” §7023(i) (emphasis added).

No provision of the CCPA, even as modified by the CPRA, requires businesses to disclose specific sources of personal information. See §§1798.106, 110(a)(2), 130(a)(3)(B)(ii), 130(a)(B)-(C), 130(a)(5)(B)(ii). The CCPA's right to know requires only the disclosure of categories of sources from which personal information is collected, not specific sources. See §1798 at 110(a)(2). Complying with the CPRA's right to correct requires only that the business correct the inaccurate information and does not require businesses to disclose any information to consumers, other than notifying consumers

that the right to correct exists. See *id* at 106. The draft Regulations expand the right to correct under the CPRA by requiring businesses to disclose specific sources “in addition to processing the consumer’s request [to correct].” §7023(i) (emphasis added).

b. Necessity

Furthermore, disclosing a specific source of personal information is not necessary to effectuate the purpose of the right to correct under the CPRA. Per the statute, the CPRA’s right to correct requires a business to “use commercially reasonable efforts to correct the inaccurate personal information” the business maintains. §1798.106. Section 7023(c) of the proposed Regulations already expands the statutory obligation by requiring that a business receiving a request to correct “shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected,” but the additional requirement to maintain correction is arguably logical and necessary to effectuate the correction right. On the contrary, the obligation imposed in subdivision (e) that requires disclosure of the source(s) even if the business is otherwise able to correct the information and ensure that it remains corrected in its own systems is unnecessary to effectuate the right to correct.

3. Recommended Revisions to Regulations Section 7023(i)

We propose two alternatives to modify subdivision 7023(i) of the draft Regulations to effectuate the purpose of the statute in a less burdensome and more accurate way. First, strike the subdivision in its entirety. Given the inconsistencies between subdivision (i) and the CPRA text and obligations, and the unnecessary nature of this language, striking the provision in its entirety is the preferred alternative.

Second, add a modified version of the section to section 7023(c), tied to the obligation to ensure that corrected information remains corrected, as follows: (text added shown in blue, remainder of paragraph, stet.):

“A business that complies with a consumer’s request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. **Where the business is unable to ensure that the inaccurate information remains corrected, due to the nature of the method by which, or the source from which the business receives information, the business shall, in addition to correcting the personal information at issue in its existing systems, provide the consumer with the name of the source from which the business received the alleged inaccurate information. . . .**”

Although the second proposed alternative may still be somewhat inconsistent and unnecessary despite the modifications, a business should only be required to disclose the specific source of inaccurate personal information if it is unable to correct or maintain the correction of factually incorrect information.

Respectfully submitted.

From: **Kevin Gould** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment -- CPPA CPRA Proposed Regulations Comment Letter
Date: 23.08.2022 20:17:59 (+02:00)
Attachments: CPPA CPRA Proposed Regulations Comment Letter.pdf (8 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Thank you for the opportunity to provide comments on the proposed rulemaking implementing the California Privacy Rights Act of 2020. Please let us know if you have any questions regarding our attached comment letter. Thank you.



Kevin Gould
EVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
T: [REDACTED]
F: [REDACTED]
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)



August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Boulevard
Sacramento, CA 95834
regulations@coppa.ca.gov

RE: Comments on Proposed Rulemaking Implementing the California Privacy Rights Act of 2020

Dear Mr. Soublet:

The California Bankers Association (CBA) appreciates the opportunity to submit comments to the California Privacy Protection Agency (Agency) on the proposed rulemaking to adopt regulations to implement the California Privacy Rights Act (CPRA) of 2020. CBA is one of the largest banking trade associations in the United States advocating on legislative, regulatory, and legal matters on behalf of banks doing business in California.

The importance of protecting consumer data and privacy are not new concepts for banks who have operated for decades under protections established by laws like the Gramm-Leach-Bliley Act and California Financial Information Privacy Act. As the Agency works toward adopting regulations in accordance with the CPRA, we appreciate the opportunity to provide input.

Section 7002: Restrictions on the Collection and Use of Personal Information.

Section 7002(a) requires “explicit consent” to collect, use, retain, or share personal information for “any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed.” To the contrary, Civil Code Section 1798.100(a)(1) permits the collection or use of personal information for additional purposes that are incompatible with the disclosed purposes as long as the business notifies the consumer of the additional purposes. Accordingly, we believe requiring “explicit consent” goes beyond the statute. We urge that the regulations be consistent with the statute by requiring notice, not explicit consent.

Section 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

Section 7004(a)(5) requires that California Consumer Privacy Act (CCPA) requests submitted by consumers be easy to execute. While understandable, making technical issues like broken links a violation of the regulation is excessive and unduly burdensome. We request that this language be removed or that a willful or malicious intent standard be included when imposing liability for a broken link.

Section 7004(c) states that a “user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent.” The proposed regulations subject businesses to strict liability regarding the development and implementation of their user interfaces. As such, the Agency could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that are accidental.

Businesses may experience problems with their user interfaces. These problems may occur without the business’s negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminals can alter or disrupt a business’s online presence despite the business’s best efforts. A business should not be punished for something that was unintentional, that it did not cause, nor for something it could not prevent. Instead of strict liability, the regulations should consider the business’s intent, knowledge, and other relevant factors, such as information security practices. The proposed regulations also fail to make it clear what qualifies as substantial.

Section 7010: Overview of Required Disclosures.

Section 7010(b) of the proposed regulations require a “business that controls the collection of a consumer’s personal information shall provide a notice at collection.” The proposed regulations delete the reference to collecting personal information “from a consumer” suggesting that the notice must cover personal information obtained from third parties as well as from consumers.

Conversely, Section 7012(a) indicates that the “purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them”. (Emphasis added). For consistency with Section 7012(a), the draft regulations should avoid deleting “from a consumer” in Section 7010(b).

Section 7012: Notice at Collection of Personal Information.

Section 7012(e)(4) requires the notice at collection of personal information to include the “length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will

be retained.” We urge that this provision be removed or that it allow flexibility. Aside from being difficult to comply with, a lengthy and complicated notice is less likely to be read by consumers compared to a more basic notice that indicates how personal information is collected and used.

Section 7012(e)(6) requires a business to include in its notice at collection if the “business allows third parties to control the collection of personal information, the names of all third parties; or, in the alternative, information about the third parties’ business practices.” Conversely, Civil Code Section 1798.110(c)(4) requires a business that collects personal information about consumers shall disclose the “categories of third parties to whom the business discloses personal information.” As such, the statute doesn’t require a business to disclose the names of third parties nor the third party’s business practices as proposed by the regulations. The proposed regulations go beyond the statute. Accordingly, we urge that the regulations be consistent with the statute by requiring disclosure of the categories of third parties, not the names or business practices of third parties.

Section 7022: Requests to Delete.

Section 7022(c)(4) requires a service provider or contractor, upon notification by a business, to notify any other service providers, contractors, or third parties to delete the consumer’s personal information unless it is impossible or involves disproportionate effort. If the service provider or contractor claims that such a notification involves a disproportionate effort, “the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort.”

We urge that the requirement to provide a detailed explanation be removed given that this requirement is not derived from the statute and considering the complexity and the resource intensive nature that would be involved in determining whether providing a notification involves a disproportionate effort.

Section 7023: Requests to Correct.

The proposed regulations create new requirements around requests to correct that make compliance operationally and technically infeasible. More specifically, the proposed regulations in Section 7023(c) require that a business must ensure that personal information remain corrected, which could require a business to establish mechanisms ensuring that corrected personal information is not overridden by inaccurate personal information subsequently received. Another example is in Section 7023(i) of the proposed regulations, which requires that a business must not only correct personal information, but it must provide the consumer with the name of the source of the alleged inaccurate information where the business itself is not the source of the information.

When responding to a request to correct, Section 7023(f)(2) requires a business that claims complying with the request to correct is impossible or would involve a disproportionate effort to provide the “consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request.”

We urge that the requirement to provide a detailed explanation be removed given that this requirement is not derived from the statute and considering the complexity and the resource intensive nature that would be involved in determining whether complying with the request to correct involves a disproportionate effort.

Section 7023(f)(3) requires a business that has denied a consumer’s request to correct in whole or in part, to inform “the consumer that, upon the consumer’s request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer”, unless the request is fraudulent or abusive. This requirement goes beyond the statute, and we request that the provision be removed. Further, if the denial is lawful, it is unclear what the person will do with this information.

Section 7023(h) requires a business that determines that a request to correct is fraudulent or abusive must “inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.” This provision should be removed from the proposed regulations as it raises a security risk for consumers by potentially revealing anti-fraud protocols to potential wrongdoers.

Section 7025: Opt-Out Preference Signals.

Section 7025(b) states that a “business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing”, which is inconsistent with Civil Code Section 1798.135(b)(3), which states that a “business that complies with subdivision (a) is not required to comply with subdivision (b).” Civil Code Section 1798.135(a) outlines the requirements for businesses that provide opt-out links on its internet homepage.

Civil Code Section 1798.135(b)(3) states for “the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).” Accordingly, the statute grants businesses the choice of whether they want to provide opt-out links on their internet homepage or honor universal opt-out preference signals.

Conversely, the proposed regulations require businesses to provide opt-out links on their internet homepage and to honor universal opt-out preference signals. We urge that the regulations align with the statute, thereby permitting businesses the option granted in statute.

Section 7026: Requests to Opt-Out of Sale/Sharing.

Section 7026(f)(2) requires a business to comply with a request to opt-out of the sale or sharing of personal information by notifying “all third parties to whom the business has sold or shared the consumer’s personal information” of the consumer’s request to opt-out of the sale or sharing and to forward the consumer’s opt-out request to “any other person with whom the person has disclosed or shared the personal information.” Both of these requirements go beyond the statute and should be deleted.

Furthermore, the requirement to forward a consumer’s request to any person with whom the person has disclosed or shared the information doesn’t take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumer to make the disclosure.

Section 7027: Requests to Limit Use and Disclosure of Sensitive Personal Information.

Civil Code Section 1798.121(d) states that sensitive personal information “that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.”

The proposed regulations focus on the request to limit the use and disclosure of sensitive personal information but do not offer clarity on when sensitive personal information is considered collected or processed. According to the statute quoted above, collecting or processing sensitive personal information for purposes other than inferring characteristics about a consumer is exempt from the right to limit the use and disclosure of sensitive personal information. However, the proposed regulations imply this exemption does not exist and any collection or processing of sensitive personal information is subject to the right to limit its use and disclosure. The regulations should be amended to align with the statute.

In addition, the draft regulations provide seven permissible uses of sensitive personal information. However, these permissible uses should be clarified and expanded to include uses of sensitive personal information to comply with legal or regulatory obligations.

Section 7050: Service Providers and Contractors.

The proposed regulations provide a limited view of the types of advertising services that may be provided by service providers and contractors. Under the proposed regulations and illustrative examples, a social media company that acts as a service provider or contractor cannot use a list

of a business's customer email addresses to identify users on the social media company's platform to serve advertisements to them.

The proposed regulations do not address a circumstance where the social media company agrees to use personal information solely for the business's benefit, in which case the social media company would be operating as a service provider or contractor. Without further clarification in the regulations, situations where businesses disclose personal information to an entity solely to provide services to the business could constitute sharing under the CPRA when no cross-context behavioral advertising occurs.

Section 7051: Contract Requirements for Service Providers and Contractors.

The proposed regulations in Section 7051(a)(2) require that agreements between a business and service provider or contractor identify specific purposes for which personal information is disclosed, which cannot be described in "generic terms, such as referencing the entire contract generally." This provision requires businesses to take a highly customized approach to every engagement that utilizes a standard addendum to address data usage restrictions in compliance with the law. Requiring businesses to take a customized approach to every engagement is overly burdensome to businesses without providing a commensurate benefit to the consumer and we believe that the provisions go beyond statutory requirements.

Section 7051(e) states that whether "a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations." The section offers an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intended to use the personal information in violation of the CCPA.

This provision goes beyond the statute and shifts service provider and contractor liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent this shift in liability. We urge the striking of these provisions or clarifying them such that businesses have clear guidance on what level of due diligence is required to prevent liability.

Section 7053: Contract Requirements for Third Parties.

Similar to the comments offered previously in Section 7051, Section 7053(a)(1) of the proposed regulations require that a business identify, in each agreement, the specified purpose for which personal information is sold or disclosed, which goes beyond the statutory requirements.

Section 7053(e) states that whether “a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations.” The section offers an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the third party intended to use the personal information in violation of the CCPA.

This provision goes beyond the statute and shifts third party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent this shifting of liability. We urge the striking of these provisions or clarifying them such that businesses have clear guidance on what level of due diligence is required to prevent liability.

Section 7063: Authorized Agents.

Civil Code Section 1798.185(a)(7) requires rules and procedures to facilitate a consumer’s authorized agent to make various CCPA-related requests taking into consideration, among other things, security concerns.

We continue to underscore our concerns that the regulations pertaining to authorized agents may provide an opportunity for fraud by allowing a consumer to authorize an agent to manage their personal information based on a signature and without a requirement for the agent to be registered or for the consumer to provide a power of attorney or a notarized signature.

Section 7304: Agency Audits.

With respect to the Agency’s authority to audit businesses’ compliance with the law, we urge the Agency to exempt banks which are highly regulated and subject to ongoing supervision and frequent examination by banking regulators.

State and federally chartered banks have at least three independent regulators. For example, state-chartered banks are presently regulated by the California Department of Financial Protection and Innovation, the federal Consumer Financial Protection Bureau, and the Federal Deposit Insurance Corporation (FDIC). This level of oversight includes frequent, routine examinations by regulatory agencies of not only the safety and soundness of these organizations but of their compliance with various laws whether focused on consumer protection or otherwise.

Bank examinations are comprehensive and require a bank to dedicate significant time and resources in advance of the exam commencing. Banks are required to gather and compile significant amounts of records, data and information in preparation for an examination. While examiners may conduct some portion of an exam off-site it is typical that the regulator conducts

California Privacy Protection Agency
Comments on Proposed Rulemaking
California Privacy Rights Act of 2020
August 23, 2022
Page 8

a portion of the examination on bank premises. Examinations conclude with the regulator communicating findings to the bank through meetings with management and an exam report.

With respect to the adherence to state and federal laws, banking regulators are granted broad authority when conducting compliance exams. As an example, the FDIC's Consumer Compliance Examination Manual requires the examiner to review the bank's compliance with the Gramm-Leach-Bliley Act. In this regard, the examiner is considering the bank's notices, privacy policies, internal controls, information sharing practices, complaint logs, administration of opt-out requests, etc. Similarly, the California Department of Financial Protection and Innovation examines a bank's compliance with the California Financial Information Privacy Act.

In furtherance of our request that banks be exempt from audit, the Agency may wish to familiarize itself with the comprehensive processes and systems developed by bank regulators surrounding routine examinations, including the detailed examination manuals that are publicly available. We urge the Agency to consider the robustness of bank examinations, the well-developed structure that has been established around exams, the extensive scope of the review covered in an exam, and the routine and frequent nature in which these exams are conducted.

Enforcement Deadline.

Understanding that final regulations will not be adopted by the statutorily mandated deadline of July 1, 2022, as required by Civil Code Section 1798.185(d), we request that the regulations not be enforceable until one year from the date of final adoption of this rulemaking. Businesses subject to the CPRA would have been given one year to implement the requirements of the regulations before enforcement of the regulations began. Accordingly, we request that the regulations become enforceable one year after the date the regulations are finalized.

####

Thank you for the opportunity to offer comments. We welcome any questions you may have.

Sincerely,



Kevin Gould
EVP/Director of Government Relations

KG:la

From: **Travis Frazier** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Christopher Oswald** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 20:21:14 (+02:00)
Attachments: FINAL ANA Comments on Proposed CPRA Regulations (Aug. 23, 2022).pdf (21 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see attached for comments from the Association of National Advertisers (ANA) regarding the proposed regulations to implement the CPRA.

Regards,

Travis Frazier

Manager, Government Relations | [ANA](#)

P: [REDACTED] | [ana.net](#) | [@ANAGovRel](#) | [LinkedIn](#)

2020 K Street, NW, Suite 660, Washington, DC 20006

The ANA drives growth for you, your brand, our industry, and humanity. Learn how at [ana.net/membership](#).



**Before the
CALIFORNIA PRIVACY PROTECTION AGENCY
Attn: Brian Soublet
2101 Arena Blvd., Sacramento, CA 95834
Email: regulations@coppa.ca.gov**

COMMENTS

of the

ANA – ASSOCIATION OF NATIONAL ADVERTISERS

on the

**Text of Proposed Regulations to Implement
the California Privacy Rights Act of 2020
CPPA Public Comment**

Christopher Oswald
EVP, Head of Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC 20006
[REDACTED]

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
[REDACTED]

August 23, 2022

On behalf of ANA – Association of National Advertisers (“ANA”), we provide comments in response to the California Privacy Protection Agency’s (“CPPA” or “Agency”) July 8, 2022 request for public comment on the text of proposed regulations to implement the California Privacy Rights Act of 2020 (“CPRA”).¹ The ANA fully supports the goal of advancing strong and meaningful privacy protections for Californians, but we are concerned that certain provisions in the proposed regulations would hinder—rather than advance—consumer privacy and choice, and other provisions would conflict with the clear language, mandates, and intent of the CPRA itself. We therefore provide these comments to help the Agency better conform the proposed regulations to the law.

The mission of the ANA is to drive growth for marketing professionals, brands and businesses, the industry, and humanity. The ANA serves the marketing needs of 20,000 brands by leveraging the 12-point ANA Growth Agenda, which has been endorsed by the Global CMO Growth Council. The ANA’s membership consists of U.S. and international companies, including client-side marketers, nonprofits, fundraisers, and marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and vendors). The ANA creates Marketing Growth Champions by serving, educating, and advocating for more than 50,000 industry members that collectively invest more than \$400 billion in marketing and advertising annually. Our members include small, mid-size, and large firms, and virtually all of them engage in or benefit from data-driven advertising practices that give consumers access to relevant information, messaging, and advertisements at the right time and in the right place.

ANA provided California’s government with input at nearly every stage in the California Consumer Privacy Act of 2018’s (“CCPA”) development. We testified in person at legislative and administrative hearings, submitted written comments on the content of the draft CCPA regulations, held discussions with government staff, and closely followed the changes to the CCPA through the legislative and regulatory process. With the transfer of regulatory authority to the Agency, we will continue our engagement with the CPPA Board and staff, Executive Director, and other California government leaders to advance the critically important subject of consumer privacy. We therefore welcome the release of draft regulations to implement the CPRA for public comment.

However, as an overarching, threshold matter, we are deeply concerned that the proposed regulations would substantially and materially alter statutory requirements in the CPRA’s text, thus substituting a regulator’s extra-legislative objectives for the specific language of the law. The ANA and our members support the Agency’s goal to provide Californians with improved privacy protections, but the proposed rules implementing the CPRA contain many provisions that substantively change businesses’ obligations as set forth in the law. The CPRA’s implementing regulations can only be promulgated within the legal authority granted to the CPPA. While we recognize that the proposed regulations are in “draft” form, several of the proposed rules are obviously *ultra vires* and contravene the law by creating requirements that are significantly different from, and in some cases diametrically opposed to, the CPRA’s requirements (as described in more detail in these comments). We therefore urge you to consider

¹ CPPA, *Notice of Proposed Rulemaking* (Jul. 8, 2022), located [here](#).

these comments and modify the proposed regulations so they align with the text and intent of the statute.

Additionally, we are particularly concerned that the Economic and Fiscal Impact Statement (“EFIS”) to support the proposed regulations severely underestimates the costs associated with the draft rules.² For example, the EFIS states that “the proposed regulation has a small cost per business,” (\$128) when actual studies have shown that the cost of executing just a single consumer rights request under the CCPA can reach \$1,500.³ Given that the CPRA creates new consumer rights associated with sensitive personal information and personal information correction, costs of compliance are almost certainly likely to be greater than \$128 per business. Similarly, the EFIS states that the proposed regulations are expected to increase labor hours required for CCPA compliance by just 1.5 hours each, while reports have shown “[o]rganizations spend an average of 60 to 130 person hours complying with” consumer rights requests alone.⁴ The aforementioned study demonstrates that the actual cost and time required to facilitate rights requests are significant themselves. This finding does not even account for the extraordinary additional expense businesses will accrue to develop processes to meet many new requirements, including facilitating new consumer rights under the CPRA, updating required notices, and reworking contracts with customers and business partners. The EFIS should be revised to reflect the actual—and significant—costs to businesses that are associated with the proposed regulations’ mandates.

It is essential that the Agency develop a regulatory scheme that is consistent with the CPRA and that will protect consumers while also allowing businesses to continue to support and underpin what has been California’s vibrant economy. To that end, our comments address the following specific issue areas:

- I. The Agency Should Delay Enforcement of the CPRA and the Implementing Regulations for At Least One Year Following the Finalization of the Regulations**
- II. Entirely New and Subjective Proportionality Standards in the Proposed Regulations Should Be Updated to Match the CPRA**
- III. The Proposed Regulations’ Approach to Opt-Out Preference Signals Conflicts with the Text of the Law**
- IV. The Agency Should Remove Section 7050(c) of the Proposed Regulations Because It Is Unnecessary and Duplicative**
- V. The Proposed Regulations’ Symmetry of Choice Requirements Are Too Inflexible to Accommodate Different Channels and Technologies**
- VI. Forcing Businesses to Forward Opt-Out Requests Downstream Is Inconsistent with Consumer Choice and the CPRA’s Text**
- VII. Correction Requirements Should Permit Important Consumer Protections**

² CCPA, *Economic and Fiscal Impact Statement for California Consumer Privacy Act Regulations* (Jun. 28, 2022), located [here](#) (hereinafter, “EFIS”).

³ *Id.* at 2; DeAndrea Salvador, *2022 Data Privacy Trends: A CCPA Report*, DATAGRAIL (Mar. 9, 2022), located [here](#); see also Alex Woodie, *Privacy Costs Rise as CCPA Requests Jump*, DATANAMI (Mar. 11, 2022), located [here](#).

⁴ *Id.*

- VIII. The Agency Should Clarify the Proposed Regulations' Notice Requirements**
- IX. Consumer Access Requests Should Cover the Prior 12-Month Period Unless the Consumer Specifically Requests Access to Older Information**
- X. Transient, Unknown Technical Violations of the Regulations Should Not Be Grounds for Enforcement**
- XI. The Data-Driven and Ad-Supported Online Ecosystem Benefits California Residents and Fuels Economic Growth**

ANA thanks you for the opportunity to provide comments on the proposed regulations and looks forward to continuing to engage with you throughout the regulatory process.

* * *

I. The Agency Should Delay Enforcement of the CPRA and the Implementing Regulations for At Least One Year Following the Finalization of the Regulations

The CPRA specified the statutory deadline for the Agency to issue *finalized* regulations implementing the statute as July 1, 2022.⁵ Unfortunately, this deadline passed before the Agency released the proposed CPRA implementing regulations for formal comment. Had the Agency met the CPRA’s statutory deadline for final rules, businesses would have had (as intended by the statute) a full year to come into compliance with regulatory requirements prior to civil and administrative enforcement of the CPRA (scheduled to begin on July 1, 2023).⁶ Indeed, the text of the CPRA contemplates a one-year period for businesses to bring themselves into compliance with the law’s new mandates and its associated regulations prior to facing enforcement, and so the Agency should forebear from enforcing the CPRA or its implementing regulations until at least one year after the date the regulations are finalized (*i.e.* approved by the California Office of Administrative Law, filed with the California Secretary of State, and officially made effective pursuant to the quarterly effective date schedule for regulations under California law).⁷

The Agency’s proposed changes to the regulatory framework in effect under the CCPA are significant. The proposed regulations implement the CPRA, a law that substantially and materially amended the CCPA upon its approval by California voters via ballot initiative in 2020. Businesses cannot begin to take meaningful, concrete steps towards compliance with the CPRA regulations until they are finalized; otherwise, businesses may invest significant resources to meet requirements that could materially and substantively change prior to being finalized. Businesses need ample time to develop processes that adhere to the regulations’ requirements for the CPRA’s new consumer rights, gain clarity on the CPRA’s notice and choice mandates, and perform the due diligence and governance functions required by the CPRA before being penalized for violations. We therefore ask you to delay enforcement until at least one year following the effective date of the proposed regulations. Such a compliance ramp-up period—namely, at least one year following the effective date of final regulations—was envisioned by the CPRA and is necessary to allow businesses sufficient time to comply with the final rules.

II. Entirely New and Subjective Proportionality Standards in the Proposed Regulations Should Be Updated to Match the CPRA

The proposed regulations, through illustrative examples as well as plain text, include novel and ambiguous proportionality standards and requirements that directly conflict with the CPRA itself. As described in more detail below, the proposed rules inject a new subjective “average consumer expectation” standard into the law’s “necessary and proportionate”

⁵ Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023) (“Notwithstanding subdivision (a), the timeline for adopting final regulations required by the Act adding this subdivision shall be July 1, 2022.”)

⁶ *Id.* (“Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this Act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date.”)

⁷ Cal. Gov. Code, §§ 11349.3(a), 11349.4(a) (describing the typical timeline for the California Office of Administrative Law (“OAL”) to review agency-drafted regulations and submit them to the California Secretary of State, and discussing the quarterly schedule by which such regulations become effective depending on the date OAL files them with the California Secretary of State).

requirements that provides no guidance to businesses about permissible uses of personal information. The proposed regulations also create opt-in consent requirements where the CPRA clearly articulates an opt-out approach. The Agency should amend these standards, as set forth below, to match them to the CPRA and provide needed clarity to the business community. The CPPA must not create new substantive requirements in areas where the CPRA itself already sets clear mandates.

A. The Agency Should Remove The Subjective “Average Consumer Expectation” Standard from the Regulations’ “Necessary and Proportionate” Requirements

The proposed regulations state: “a business’s collection, use, retention, and/or sharing” of “personal information” must be “reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed.”⁸ The regulations further explain that “[t]o be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with *what an average consumer would expect* when the personal information was collected.”⁹ The regulations thus introduce a subjective “average consumer expectation” standard that provides no clarity. The proposed regulations also discount the CPRA’s role of notice, which is the approach to “necessary and proportionate” use taken in the law. The Agency should remove the “average consumer expectation” standard from the regulations’ explanation of the meaning of “necessary and proportionate” data collection and use in Section 7002.

The “average consumer expectation” standard is not required for “necessary and proportionate” data collection, use, or retention under the CPRA. Instead, the CPRA ties permissible personal information collection, use, retention, sale, and sharing to consumer disclosures. The CPRA specifically permits use of personal information for a “business purpose,” defined as “the use of personal information for the business’s operational purposes, *or other notified purposes...*”¹⁰ Additionally, the CPRA’s notice at collection requirements mirror this approach to permissible data collection and use by stating that “[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes that are *incompatible with the disclosed purpose* for which the personal information was collected, without providing the consumer with notice consistent with this section.”¹¹ A similar construct and effect is also included in Section 1798.100(c) of the CPRA concerning businesses’ data retention obligations. In the same manner, the Agency has read out of law the role of notice.¹² The CPRA therefore requires businesses to disclose the purposes for data collection or use and to update applicable notices if personal information is ever collected or used for a purpose that is incompatible with the original purpose for which it was first collected.

⁸ Cal. Code Regs. tit. 11, § 7002(a) (proposed).

⁹ *Id.* (emphasis added).

¹⁰ Cal. Civ. Code § 1798.140(e) (effective Jan. 1, 2023).

¹¹ *Id.* (emphasis added).

¹² The CPRA states: “A business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, *or for another disclosed purpose* that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.” *Id.* at § 1798.100(c) (emphasis added). The CPRA thus ties necessary and proportionate use to consumer disclosures—not average consumer expectations—in multiple sections of the statute, which the proposed regulations would read out of law.

The subjective task of determining the expectation of an “average consumer” is not a prerequisite for personal information collection or use under the CPRA.

The proposed regulations’ “average consumer expectation” standard would leave businesses to guess what an “average” consumer would expect when engaging with their products or services or using the Internet. The proposed standard is inherently unclear, because businesses and consumers may reasonably differ in their ideas of reasonable consumer expectations in the marketplace. Because the “average consumer expectation” standard creates an effect that directly conflicts with the statute’s notice requirements and would add more confusion rather than clarity to the regulations, the standard should be removed from Section 7002.

B. The Proposed “Average Consumer Expectation” Standard Is Unworkable and Would Result in Outcomes That Contravene the Plain Text of the CPRA

The illustrative examples in the proposed regulations that attempt to describe an “average consumer expectation” provide little to no clarity and contravene the text of the statute. For example, one illustrative example contradicts the CPRA by imposing opt-in standards where the statute clearly takes an opt-out approach. Specifically, the illustrative example in Section 7002(b)(1) would require opt-in consent to collect “geolocation information” about a consumer who downloaded a flashlight application.¹³ Conversely, the CPRA gives consumers the right to opt out of sales and sharing of “personal information,” which includes generalized geolocation information such as zip code and hometown.¹⁴ The CPRA also provides consumers with the right to opt out of use and disclosure of “sensitive personal information,” which includes “precise geolocation” information (as defined in the CPRA).¹⁵ The CPRA thus clearly spells out an opt-out right tied to disclosure of such information. The CPRA does not restrict the collection of such data, but the CPRA regulations would impose an opt-in consent requirement for collection. The example in the proposed regulations therefore provides no clarity but, in fact, creates confusion by taking an approach diametrically opposed to the way the example would be analyzed under the clear text of the CPRA. The illustrative example thus demonstrates how the “average consumer expectation” standard found in the proposed regulations contravenes the plain text of the CPRA.

The illustrative example in Section 7002(b)(3) demonstrates the same flaw of contradicting the clear text of the CPRA. The example would prohibit Internet service providers from selling or sharing “geolocation information” to “data brokers without the consumer’s explicit consent.”¹⁶ The CPRA text suggests data brokers are “third parties” that may receive “personal information” from businesses, subject to an opt-out right for: (1) personal information sales, (2) personal information sharing, and (3) sensitive personal information use and disclosure. The CPRA contains no opt-in requirement when transfers of personal information are made to “data brokers.” The proposed regulations would usurp the CPRA’s clear statutory language regarding opt-out rights by imposing an opt-in requirement where one specifically does not exist.

¹³ Cal. Code Regs. tit. 11, § 7002(b)(1) (proposed).

¹⁴ Cal. Civ. Code §§ 1798.125, 140(v) (effective Jan. 1, 2023).

¹⁵ *Id.* at §§ 1798.121, 140(ae).

¹⁶ Cal. Code Regs. tit. 11, § 7002(b)(3) (proposed).

Because the illustrative examples inject ambiguity into the regulatory scheme rather than clarity with the “average consumer expectation” standard and contravene the clear opt-out approach taken in the law, the proposed regulatory standard itself and the illustrative examples in Sections 7002(b)(1) and 7002(b)(3) should be removed from the proposed regulations. The Agency should amend the proposed regulations so they appropriately tie permissible data collection, use, and transfers to consumer notices rather than “average consumer expectation.”

III. The Proposed Regulations’ Approach to Opt-Out Preference Signals Conflicts with the Text of the Law

According to the proposed regulations, “[w]hen a business that collects personal information from consumers online receives or detects an opt-out preference signal... [t]he business shall treat the... signal as a valid request to opt-out of sale or sharing...”¹⁷ This proposed rule contravenes the CPRA, which makes businesses’ adherence to such signals optional. The proposed regulations also ignore the CPRA’s clear regulatory directive for the Agency to issue rules defining key safeguards for the development of such optional opt-out preference signals. The Agency should therefore remove Sections 7025(c) and (e) from the proposed regulations and first address the statutorily required rulemaking regarding safeguards for opt-out preference signals.

A. The Agency Should Align the Regulations With the CPRA, Which Makes Opt-Out Preference Signals Optional

According to the CPRA’s plain text, businesses “*may elect*” either to (a) “[p]rovide a clear and conspicuous link on the business’s internet homepage(s) titled ‘Do Not Sell or Share My Personal Information’” or (b) allow consumers to “opt-out of the sale or sharing of their personal information... through an opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]”¹⁸ Businesses therefore may choose either to allow consumers to opt out through a do-not-sell link on their homepage(s) or through opt-out preference signals. In direct contrast to this optional structure set forth in the text of the law itself, the Agency has proposed that adherence to opt-out preference signals is mandatory. This interpretation of the CPRA is plainly inconsistent with the clear choice outlined in the statute that allows businesses either to adhere to global signals or offer an opt-out link.

In an attempt to justify converting the clear statutory option into a mandate that businesses must honor opt-out preference signals, the Agency’s Initial Statement of Reasons (“ISOR”) does not point to the plain language of the CPRA itself, which clearly makes the opt out preference signal optional. Instead, the ISOR cites the regulatory authority section of the CPRA to defend its assertion that global privacy controls are mandatory.¹⁹ The ISOR states:

¹⁷ *Id.* at § 7025(c)(1).

¹⁸ Cal. Civ. Code § 1798.135(b)(3) (effective Jan. 1, 2023) (emphasis added).

¹⁹ CPPA, *Initial Statement of Reasons* at 34-35, located [here](#).

This regulation is also necessary to address a common misinterpretation of Civil Code section 1798.135, subdivisions (b)(3) and (e), that complying with an opt-out preference signal is optional for the business. Not so. Civil Code section 1798.135 gives the business a choice between (1) posting the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” link, or the other alternative Opt-Out link and (2) processing the opt-out preference signal in a frictionless manner in accordance with the regulations. (See Civ. Code, § 1798.135, subd. (b)(1) (referencing technical specifications described in Civil Code section 1798.185, subdivision (a)(20), about a frictionless processing of the signal, and not subdivision (a)(19), regarding the opt-out preference signal generally.) Whether or not the business posts the opt-out links, the CPRA amendments to the CCPA require a business to always comply with an opt-out preference signal.²⁰

This explanation imports an entirely new, extralegal concept of “frictionless manner” into the CPRA, even though the statute itself contains no such verbiage or concept. The Agency adds that, to be free from the requirement of providing an opt-out link, businesses must honor opt-out preference signals in a “frictionless manner” or they must provide an opt-out link *and* honor such signals in a “non-frictionless manner.”²¹ The term “frictionless manner” is defined by the Agency to mean honoring signals without charging a fee, changing a consumer’s experience with a product or service, or displaying a notification in response to an opt-out preference signal.²² The CPPA consequently contradicts the CPRA’s flexible approach of giving businesses options for processing opt-out requests by mandating honoring opt-out preference signals, even if businesses have decided to provide an opt-out link.

The ISOR’s reasoning also ignores the fact that the regulatory directive section (Section 1798.185(a)(20)) itself actually references the *optional* nature of opt-out preference signals by setting forth a clear regulatory directive that the CPPA must issue “regulations to govern how a business that has *elected* to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal....”²³ The Section requires the Agency to issue rules governing how businesses that have *elected* to respond to opt-out preference signals (and not provide an opt-out link) must respond to those signals. The preceding section (Section 1798.185(a)(19)) sets forth a clear directive for the Agency to promulgate “technical specifications” (which typically describe the core idea and goals of a given software product) to govern the optional signals. The regulatory authorities in Section 1798.185(a)(19) and (a)(20) thus work together. Subsection (a)(19) requires the Agency to set the goals and core ideas behind the optional opt-out preference signal by promulgating technical specifications, and subsection (a)(20) directs the Agency to issue rules governing how a business must respond to these new signals in the event it chooses to accept them.

The CPRA is a statute that Californians approved directly by affirmatively voting it into law through their ballots. The Agency’s misinterpretation of the clear option for businesses either to adhere to opt-out preference signals or offer an opt-out link consequently defies what Californians voted into law in November 2020. The Agency should remove Sections 7025(c)

²⁰ *Id.*

²¹ Cal. Code Regs. tit. 11, § 7025(e) (proposed).

²² *Id.* at §§ 7001(m), 7025(f).

²³ Cal. Civ. Code § 1798.185(a)(20) (effective Jan. 1, 2023) (emphasis added).

and (e) from the proposed regulations in order to conform to the CPRA’s option for companies either to provide an opt-out link or accept opt-out rights through a preference signal.

B. The Agency Should Define Key Safeguards to Guide Opt-Out Preference Signals

While the proposed regulations impose a conflicting requirement where a clear option is present in the law, they fail to address important provisions of the CPRA that are intended to guide and protect the creation of opt-out preference signals. The CPRA tasks the Agency to issue particularized opt-out preference signal regulations so as to ensure such controls are true expressions of consumer choice rather than being set by default by intermediaries. For example, the CPRA states the Agency’s opt-out preference signal requirements “should... clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent.”²⁴ Additionally, the regulations section of the CPRA tasks the Agency with issuing rules to “ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.”²⁵ These safeguards—which the Agency is specifically directed to consider and issue regulations to effectuate—are nowhere present in the proposed draft regulations. Without the Agency’s acknowledgement and development of these key safeguards surrounding global signals, consumers are at risk that choices will be made for them by parties that do not consult consumers first. Intermediary companies that stand between consumers and businesses should not be permitted to decide how the consumer experiences the Internet absent the consumer’s affirmative choice. The Agency should issue regulations to clarify and define the key safeguards set forth in Section 1798.185(a)(19)(A) of the CPRA.

IV. The Agency Should Remove Section 7050(c) of the Proposed Regulations Because It Is Unnecessary and Duplicative

Section 7050(c) should be removed from the draft regulations, as it is unnecessary and duplicative. The proposed regulation is a restatement of the CPRA restriction that an entity cannot provide cross-context behavioral advertising (“CCBA”) services as a service provider.²⁶ The proposed regulation also restates the CPRA by affirming that an entity may provide advertising and marketing services as a service provider and, subject to an opt-out, even combine personal information in certain circumstances for advertising and marketing purposes.²⁷ This text is duplicative of proposed regulation Section 7050(b)(4). The CPRA is sufficiently clear with respect to entities engaged in CCBA as third parties and makes clear that it is CCBA itself (the targeting of an advertisement based on data combined from multiple businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts) that constitutes prohibited service provider activity, not advertising and marketing services generally. Therefore, Section 7050(c) is unnecessary and should be removed from the proposed regulations.

²⁴ *Id.* at § 1798.185(a)(19)(A)(iii).

²⁵ *Id.* at § 1798.185(a)(19)(A)(i).

²⁶ Cal. Code Regs. tit. 11, § 7050(c) (proposed).

²⁷ *Id.*

V. The Proposed Regulations' Symmetry of Choice Requirements Are Too Inflexible to Accommodate Different Channels and Technologies

The proposed regulations would require “symmetry of choice”—*i.e.*, the number of steps necessary for consumers to exercise choices to be the same regardless of what the choice entails.²⁸ Instead of mandating perfect symmetry in the number of steps consumers must take to exercise choices, the regulations should require businesses to exercise a reasonable effort to provide symmetry for consumer choice paths.

The Agency should not require exact symmetry because exact symmetry is likely not possible or advantageous for consumers in all instances, given differences in technology or the choices themselves. Consumers should not be deprived of the ability to receive pertinent information about their privacy choices or to benefit from measures businesses may employ to educate consumers about the results of certain choices. A standard that requires businesses to make reasonable efforts to ensure choice paths contain relatively the same number of steps, instead of exactly the same number of steps, would strike a better balance of ensuring consumers can efficiently exercise choices while providing flexibility for businesses to execute a request effectively and safely.

The proposed regulations' illustrative example in Section 7004(a)(2)(A) mandates that the process for submitting an opt-out request to a business should not involve more steps than a request to opt in. This example ignores the reality that the steps a consumer must take to effectuate a choice may be different depending on the kind of channel or type of technology they are using. For example, the user interface for a smart speaker may require more steps for users to make choices or may require them to use other mediums, like an app-based portal, to modify settings. Consequently, the choice path for smart speakers may reasonably differ from the choice path for a service that is available only via a mobile application interface.

Moreover, mechanisms may be asymmetric to give consumers numerous logical paths for exercising choice. Consumers may be permitted to make the same choices in multiple ways, some of which may involve fewer steps than others. For example, across certain major mobile operating systems, to permit the collection of location data via an app, a consumer is currently offered an in-app prompt upon opening the application to permit access to location data via a single click (just-in-time choice). The same operating systems also offer consumers additional means to modify location data permissions via the device settings, which are available to consumers through multiple clicks. Regulations that do not account for differences across channels, devices, and other modes of interactions between businesses and consumers risk hindering consumer choice and companies' ability to provide innovative technologies and logical choice paths that effectively enable consumers to express preferences through different interfaces. The Agency should revise the draft regulations to require businesses to make reasonable efforts to achieve choice path symmetry rather than issue a one-size-fits-all requirement for symmetry of choice.

²⁸ *Id.* at § 7004(a)(2).

VI. Forcing Businesses to Forward Opt-Out Requests Downstream Is Inconsistent with Consumer Choice and the CPRA’s Text

The CPRA regulations would require businesses to forward opt-out requests to other parties in the ecosystem²⁹—a requirement not found in the text of the CPRA itself. Additionally, the requirement could be misaligned with consumer choices. When a consumer submits an opt-out request to one business via a “Do Not Sell or Share My Personal Information” button, the consumer is indicating an intent to opt out of that one business’s sales and/or sharing of personal information. When clicking the button, the consumer is not expressing a preference that the business forward the opt-out selection to others in the marketplace. Because the requirement to forward opt out requests downstream is inconsistent with the text of the CPRA and consumer choices, the Agency should remove this requirement from the proposed regulations.

The CPRA is clear on the scope and intent of consumer rights. For example, the CPRA explicitly requires companies to forward deletion requests to third parties and service providers.³⁰ The CPRA states: “A business that receives a verifiable consumer request for a consumer to delete the consumer’s personal information... shall... notify any service providers or contractors..., and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer’s personal information, unless this proves impossible or involves disproportionate effort.”³¹ The CPRA does not include a similar mandate with respect to opt-out requests. The lack of a statutory requirement for businesses to forward opt-out requests to others in the ecosystem, when such a requirement explicitly exists for other rights, suggests the drafters of the CPRA did not intend to require opt-outs be sent to other businesses.

Additionally, requiring companies to forward a consumer opt-out request to other businesses would have unintended impacts for consumers. If a consumer clicks a “Do Not Sell or Share My Personal Information” link on a sports apparel website, the consumer likely does not want parties with which the sports apparel company shares personal information—such as third party rewards companies—to opt the consumer out of data transfers. Consumer choices to opt out of personal information sales and sharing are served on individual companies for reasons that are specific and unique to each consumer. By making a single choice with respect to one company’s ability to transfer data, consumers do not intend to submit an opt-out request that is effective throughout the entire Internet marketplace. For these reasons, the Agency should remove the *ultra vires* requirement to forward opt-out requests to other businesses in Section 7026(f)(2) & (3) of the proposed regulations.

VII. Correction Requirements Should Permit Important Consumer Protections

The proposed regulations’ requirements surrounding the new consumer right of correction, while well-intentioned, could inadvertently impair businesses’ ability to detect fraud. The proposed rules could also make it easier for fraudsters to gain access to others’ personal information. The Agency should therefore carefully consider how the present correction

²⁹ *Id.* at §§ 7026(f)(2) & (3).

³⁰ Cal. Civ. Code § 1798.105(c)(1) (effective Jan. 1, 2023).

³¹ *Id.*

regulations could unintentionally enable fraud and change the proposed rules accordingly to ensure personal information can be appropriately protected from misuse.

Several of the proposed regulations' mandates surrounding the correction right could facilitate fraudulent requests to the detriment of consumers and society. For example, the proposed regulations state that, if a business does not maintain documentation to support the accuracy of the information it has on file, the consumer's assertion of inaccuracy alone could be enough to establish the personal information is inaccurate.³² It is not standard business practice for companies to maintain documentation that attests to the accuracy of the data they process. The regulations suggest that a lack of such back-up documentation could empower any consumer correction request to be effectuated, even if the information the business maintains is actually accurate. The Agency should remove Section 7023(b)(2) from the proposed regulations to protect consumers from fraudulent correction requests.

Moreover, businesses regularly purposefully maintain inaccurate information and associate it with consumers or their accounts in order to detect fraud patterns. For example, if a fraudster attempts to access a user's account but misspells the user's login credentials, a company may keep a record of that misspelling to enable it to detect the same misspelling later. That activity allows the company to more quickly and easily ensure the user's account is secure and notify the real user of the attempted fraudulent access to their information. Maintaining inaccurate information on file in order to better protect consumers is a common business practice based on legitimate purposes.

Another example of a proposed correction rule that could inadvertently empower fraud is Section 7023(j)'s requirement for businesses, upon request, to provide specific pieces of personal information back to the requestor to allow them to "confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct."³³ This provision, taken together with the permissive approach to correction requests in Section 7023(b)(2), could embolden fraudsters to use correction requests to gain access to specific pieces of personal information about a particular individual. A study in the EU examined and documented the ways in which fraudulent privacy requests and prescriptive legal requirements surrounding the processing of such requests can negatively impact consumers.³⁴ The study's authors were able to use social engineering tactics to exploit businesses' privacy rights request systems to access others' personal information. As presently drafted, the proposed rules' correction mandates could empower nefarious individuals or entities to submit fraudulent requests to companies and obtain information they should not be able to access. The Agency should consequently remove Section 7023(j) of the proposed regulations and conduct a holistic review of its proposed correction right regulations to ensure the rules do not unintentionally make it easier for individuals to submit fraudulent requests.

³² Cal. Code Regs. tit. 11, § 7023(b)(2) (proposed).

³³ *Id.* at § 7023(j).

³⁴ James Pavur & Casey Knerr, *GDPArrrrr: Using Privacy Laws to Steal Identities*, BLACKHAT USA (2019), located [here](#) (considering how legal ambiguity surrounding the GDPR's access right could be abused by social engineers).

VIII. The Agency Should Clarify the Proposed Regulations' Notice Requirements

Several proposed requirements involving consumer notices should be clarified to provide more useful and digestible information to consumers. In particular, the proposed regulations' requirements for affirmative statements in privacy policies, notices regarding offline data practices, and notices on connected devices should be streamlined and clarified as set forth below.

A. The Regulations Should Not Force Businesses to Make Affirmative Public Statements Regarding Information They May Not or Cannot Know

The proposed regulations would require businesses to make affirmative statements regarding children in their privacy policies. According to the proposed regulations, businesses must publicly state whether they have actual knowledge that they sell or share personal information of consumers under age 16.³⁵ This mandate adds an entirely new element, as the CPRA does not require such an affirmative public statement. Rather, the CPRA prohibits businesses from selling or sharing personal information of consumers if the business has actual knowledge the consumer is less than 16 years of age.³⁶ Despite businesses' best efforts, the proposed regulations' affirmative privacy policy statement requirement could unreasonably subject businesses to deception claims from the Federal Trade Commission or state authorities if businesses do not update their privacy policies immediately after gaining actual knowledge that they sell or share personal information of consumers under age 16. If a rule is adopted on this subject, the CPPA should require a business to state whether it *knowingly* sells or shares personal information associated with consumers under age 16. Such a change to the proposed rules would create room for businesses that do not sell or share such personal information as a regular business activity to monitor their internal processes and rectify unintended uses of data efficiently without facing the threat of an unreasonable deception claim due to a data processing error.

B. The Regulations Should Not Require Disclosures Regarding Offline Data Practices

The Agency's proposed regulations would require a business to provide information about offline personal information collection and use practices in its online privacy policy.³⁷ Such a requirement would result in unwieldy, long, and undigestible disclosures that would not provide consumers with any real benefits. Covering the entire landscape of ways businesses may collect personal information in offline contexts would require notices containing volumes of information. Additionally, the requirement to include information about offline practices in online privacy policies represents a stark break from existing practice, which has always required businesses to provide information about online data collection and use practices in an online privacy policy. California's own California Online Privacy Protection Act and similar laws in Nevada and Delaware require privacy policies to cover only online data collection and use

³⁵ Cal. Code Regs. tit. 11, § 7011(e)(1)(G) (proposed).

³⁶ Cal. Civ. Code § 1798.120(c) (effective Jan. 1, 2023).

³⁷ Cal. Code Regs. tit. 11, § 7011(e)(1) (proposed).

practices.³⁸ The proposed regulations should be amended to remove the requirement to make disclosures regarding offline data collection and use practices.

C. The Regulations Should Permit Flexibility in Notices to Accommodate Different Kinds of Online Services and Connected Devices

The proposed regulations would require businesses to provide an opt-out notice through a connected device or in an augmented or virtual reality (“AVR”) environment “in a manner that ensures the consumer will encounter the notice” while using the device or while in the AVR environment.³⁹ These notice requirements fail to consider that such rules may significantly impair the user experience or be impossible to provide. Smart watches and smart speakers, for example, may not have the ability to provide a full opt-out notice to the consumer via their user interface. Requiring smart devices to do so could severely impair the user experience by, for example, forcing a consumer to listen to a verbatim reading of an opt-out notice before being permitted to use the smart speaker they purchased. The proposed regulations should require opt-out notices for smart devices and AVR environments to be in the primary medium used to offer the product or service, or—if the product or service is not offered in a medium that reasonably permits the required notice—another medium regularly used in conjunction with the product or service. Not all devices that generate or collect personal information will have a user interface that permits notice through the device itself (such as a smart speaker or a smart watch). If left unchanged, the proposed regulation requiring disclosures through connected devices and AVR environments could result in such devices and technologies being carved out of the digital economy because of an inability to comply with the law, resulting in less access to emerging technologies and data-supported services.

IX. Consumer Access Requests Should Cover the Prior 12-Month Period Unless the Consumer Specifically Requests Access to Older Information

The proposed regulations would require businesses to provide access to personal information beyond the 12-month period preceding the consumer’s request, even if the consumer does not specifically request access to such legacy information.⁴⁰ This requirement is inconsistent with the text of the CPRA. The draft rules should be amended to require consumers specifically to request access to information beyond the prior 12-month period, in order to match the text of the law and reduce significant operational burdens for businesses complying with access requests.

The CPRA states that, in response to an access request, “[t]he disclosure of the required information shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request, provided that... *a consumer may request* that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate

³⁸ California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575 et. seq.; Nevada Online Privacy Protection Act, Nev. Rev. Stat. §§ 603A.300 et. seq.; Delaware Online Privacy Protection Act, Del. Code Ann. tit. 6, §§ 1201C et. seq.

³⁹ Cal. Code Regs. tit. 11, §§ 7013(e)(3)(C) & (D) (proposed).

⁴⁰ *Id.* at § 7024(h).

effort.”⁴¹ The CPRA thus clearly ties the requirement to provide information beyond the prior 12-month period to a consumer’s particularized request for such legacy information. Additionally, the proposed definition of “disproportionate effort” does not provide meaningful limitations for businesses or a clear barometer by which they can determine what conduct reaches the “disproportionate effort” threshold. The draft rules should therefore be amended to make clear that a business may reasonably respond to a consumer access request by providing information that covers the 12-month period preceding the request, and only after receiving a consumer’s specific request for older information must the business provide information beyond that period.

X. Transient, Unknown Technical Violations of the Regulations Should Not Be Grounds for Enforcement

The proposed regulations would make certain passing technical violations of its provisions the potential subject of enforcement actions. For example, under the proposed regulations, “[c]ircular or broken links, and nonfunctional email addresses... may be in violation of th[e] regulation[s]” and subject to Agency enforcement.⁴² Transient technical issues such as broken links are a ubiquitous part of the Internet infrastructure. They are oftentimes quickly fixed before consumers are ever even impacted by them. Businesses should not be burdened with the risk of a CPPA enforcement action each time a privacy rights page does not render correctly, a consumer receives a faulty bounce-back email, or a privacy link is otherwise broken. Such an approach would weaponize the enforcement provisions of the CPRA into a bounty system whereby a business could be subject to a fine for a minor technical glitch. This concern is heightened by the fact that the administrative enforcement cure period will no longer be guaranteed under the CPRA.⁴³ Businesses should have flexibility to correct these technical issues swiftly without the threat of legal action. The Agency should remove Section 7004(a)(5)(B) from the proposed regulations.

The proposed regulations also include prescriptive mandates for businesses to use certain font sizes and colors for opt-out links on their websites. The regulations would require opt-out links to be in the same font size and color as other links on the business’s homepage and would require the proposed regulations’ opt-out icon to be the same size as other icons on the page.⁴⁴ In effect, these requirements could mandate that an opt-out icon must be the same size as a business’s logo on its homepage, which would impair businesses’ ability to engage in lawful commerce without providing any consumer protection benefits. Businesses should be required to make opt-out links clear and prominent, but they should have flexibility to present those links to consumers in ways that do not interfere with the business’s existing branding efforts or page aesthetics.

The proposed rules would also include certain unnecessary and prescriptive requirements regarding the presentation of consumer notices. For example, for businesses that collect personal

⁴¹ Cal. Civ. Code § 1798.130(a)(2)(B) (effective Jan. 1, 2023) (emphasis added).

⁴² Cal. Code Regs. tit. 11, § 7004(a)(5)(B) (proposed).

⁴³ Compare Cal. Civ. Code § 1798.155(b) (effective Jan. 1, 2020) with Cal. Civ. Code § 1798.155(a) (effective Jan. 1, 2023).

⁴⁴ Cal. Code Regs. tit. 11, §§ 7003(c), 7015(b) (proposed).

information online via “webforms,” a notice at collection would be required to be posted “in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.”⁴⁵ Similarly, the proposed rules would require a notice at collection to be placed on “the introductory page of the business’s website and all webpages where personal information is collected.”⁴⁶ These requirements are confusing and unnecessary, as the CPRA and proposed regulations already require privacy notices to be conspicuous.⁴⁷ The Agency should remove the requirement to post notices “in close proximity” to a webform and “on the introductory page” of a website. The Agency should also remove other prescriptive mandates in the draft rules, such as those in Sections 7003(c) and 7015(b), that place overly specific requirements on how text and images must be presented to consumers.

XI. The Data-Driven and Ad-Supported Online Ecosystem Benefits California Residents and Fuels Economic Growth

Over the past thirty years, data-driven advertising has created significant benefits by providing Californians with virtually unencumbered access to online resources and myriad opportunities for employment. Data-driven advertising has supported the existence of an open web, where consumers can access information, news, content, and online products and services at little or no cost. It has also helped to generate massive gains in United States (“U.S.”) gross domestic product (“GDP”) and has aided the stratification of economic power among companies of various sizes, resulting in small and mid-sized firms competing with the largest players in the marketplace. Overly broad regulations that unnecessarily hinder or limit data-driven advertising would harm Californians and California businesses alike. As described in more detail below, the Agency should keep the benefits provided by data-driven advertising in mind as it modifies the proposed regulations.

A. Data-Driven Advertising Drives the Economy and Employment

Data-driven advertising has created significant consumer benefits. It has generated jobs and employment opportunities for individuals that power the economy, and the growth in data-driven advertising-related economic benefits continues to compound. According to one study, the Internet economy’s contribution to U.S. GDP has grown 22 percent per year since 2016.⁴⁸ Moreover, data-driven advertising is responsible for a significant overall portion of U.S. GDP. In 2020, the Internet economy contributed \$2.45 trillion to the U.S.’s \$21.18 trillion GDP.⁴⁹ Those figures suggest that data-driven advertising is responsible for more than 10% of the total monetary value of all the goods and services produced within U.S. borders.⁵⁰

⁴⁵ *Id.* at § 7012(c)(2).

⁴⁶ *Id.* at § 7012(c)(1).

⁴⁷ *Id.* at § 7011(d).

⁴⁸ See John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU at 5 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf (hereinafter, “Deighton & Kornfeld 2021”).

⁴⁹ *Id.*

⁵⁰ See *id.*

The contributions of advertising, including data-driven advertising, to U.S. GDP are mirrored by its contributions to U.S. employment. For every million dollars spent on advertising in 2020, 83 American jobs were supported across a wide swath of industries throughout the economy.⁵¹ This figure shows that advertising, including data-driven advertising, not only serves consumers by providing relevant and useful messaging, but in a broader sense, the advertising industry serves individuals employed in industries that depend on the practice. In 2020, advertising contributed \$2.1 trillion in salaries and wages to such individuals, representing 18.2% of total labor income in the United States.⁵² The average salary for jobs ultimately supported by advertising was over \$73K, or 12% above the national average.⁵³ In reference to California specifically, one study found that the ad-supported Internet supported 1,096,407 full-time jobs across the state in 2020, more than double the number of Internet-driven jobs from 2016.⁵⁴

Presently, more than 17 million Americans are employed in jobs generated by the commercial Internet.⁵⁵ Additionally, many of these jobs have been created by small to mid-size firms rather than by large companies. In fact, in 2020 more Internet jobs were created by small firms and self-employed individuals (38 percent) than by the largest Internet companies (34 percent).⁵⁶ Moreover, consistent with the general movement of brand spending toward online media, more than half of the employment in the advertising and media fields is related to the commercial Internet, which is powered by data-driven advertising.⁵⁷

B. Data-Driven Advertising Subsidizes Californians' Access to Online Content and Consumers Prefer the Ad-Supported Model of the Internet

Data-driven advertising provides significant benefits to Californians that would not exist if the practice were significantly limited by overly prescriptive regulations. Consumers clearly benefit from data-driven advertising's support for and enablement of free and low-cost content and services that publishers offer consumers online. Without data-driven advertising, many online content and service providers may elect to adopt a subscription-based model, where content would be accessible to a consumer only upon payment of a fee. An increase in subscription-based services would change the egalitarian nature of the Internet, with consumers of means able to access cutting edge content and services while consumers with less expendable income would not be able to do so. Data-driven advertising practices allow the Internet to remain open and accessible to all by helping to make crucial content widely available for free or at a low cost.

⁵¹ See IHS Markit, *The economic impact of advertising on the US economy 2018 – 2026* at 5 (Nov. 2021).

⁵² See *id.* at 13.

⁵³ See *id.* at 5.

⁵⁴ Compare Deighton & Kornfeld 2021, at 121-123 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,096,407 jobs in 2020).

⁵⁵ Deighton & Kornfeld 2021, at 5.

⁵⁶ *Id.* at 6.

⁵⁷ *Id.* at 8.

U.S. consumers of all income levels embrace the ad-supported Internet and use it to create value in their lives. Consumers are not harmed by data-driven advertising; in fact, research shows consumers are supportive of the practice. One study found that more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.⁵⁸ Additionally, in a recent survey conducted by the Digital Advertising Alliance (“DAA”), 90 percent of surveyed consumers stated that free content was important to the overall value of the Internet, and 85 percent surveyed expressed a preference for the existing ad-supported model where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.⁵⁹ Another survey showed that consumers assign a monetary value of over \$1,400 per year to the ad-supported Internet.⁶⁰ If a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁶¹

Moreover, consumers can control data-driven advertising by opting out of the practice. In addition to the existing right to opt out of sales and sharing in the CPRA, self-regulatory frameworks such as the Digital Advertising Alliance Principles allow all consumers, regardless of their state of residency, to opt out of data-driven advertising.⁶² The DAA Principles also require companies to be transparent with consumers regarding uses of data by providing relevant notices outside a privacy policy. Such notice is often provided through the well-recognized DAA Icon that offers easy access to consumer controls for data-driven advertising.⁶³ As a result, Californians are made well-aware of data-driven advertising via the DAA Icon and can readily opt out of the practice through the DAA’s tools or the rights provided to them by the CPRA.

C. Data-Driven Advertising Promotes Competition and Supports a Vibrant Ecosystem of Companies of All Sizes, Particularly Smaller Entities

Data-driven advertising allows a flourishing ecosystem of companies to compete and contribute to a healthy economy. Data-driven advertising helps the new companies of today develop into the sophisticated, larger enterprises of the future that lend value to everyday Americans’ lives. Many different kinds of companies of various sizes, from publishers of

⁵⁸ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

⁵⁹ DAA, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

⁶⁰ DAA, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

⁶¹ Federal Trade Commission, *In re Developing the Administration’s Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁶² DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (Jul. 2009), located [here](#); FTC, *Cross-Device Tracking, An FTC Staff Report* (Jan. 2017) at 11, located [here](#) (“FTC staff commends these self-regulatory efforts to improve transparency and choice in the cross device tracking space...DAA [has] taken steps to keep up with evolving technologies and provide important guidance to their members and the public. [Its] work has improved the level of consumer protection in the marketplace.”)

⁶³ DAA, *New DAA-Commissioned Survey Shows ‘AdChoices’ Icon Recognition Has Grown to 82 Percent in 2021* (Jun. 3, 2021), located [here](#).

popular websites and small bloggers to third party ad tech companies and marketing services providers, facilitate data-driven advertising to reach individuals with relevant messaging. Third-party companies assist first-party companies looking to activate their data to reach consumers more efficiently; first-party companies rely on data-driven advertising to maximize their advertising spend; and consumers benefit from the overall practice, as they receive more relevant advertisements and broad access to information online because of the activity. All of this fosters a competitive environment.

The overwhelming majority of the companies that leverage data-driven advertising are not large platforms or market behemoths; to the contrary, they are new, small, and mid-size businesses that use, facilitate, and depend on data-driven advertising to reach their target markets and generate value. New entrants or companies with weaker market share, and therefore with less first-party data, would be substantially less able to compete if they could not use data-driven advertisements to find an audience. The wide variety of companies that engage in and benefit from data-driven advertising shows the practice serves to promote, rather than hinder, competition. Data-driven advertising creates lower barriers to entry for new market entrants, reduces small business costs, and facilitates start ups' ability to access markets. As a result, modern digital advertising is actually a fundamental driver of competition. It particularly empowers small businesses to compete where costs would otherwise hinder their market entry, leading to a greater diversity of online companies, products, and services, from which consumers gain value.

Although online publishers of all sizes rely on data-driven advertising, smaller websites depend on data-driven advertising for a significantly greater portion of their advertising revenue.⁶⁴ Data-driven advertising specifically helps small and mid-size businesses personalize their marketing, connect with the right customer segment, and therefore increase sales. One survey found that 74% of small and mid-sized businesses reported that personalized advertising was “important to the success of their business.”⁶⁵ In addition, the same study showed that, by engaging with their customers through personalized ads, small and mid-sized businesses can increase overseas sales by diversifying their customer base beyond their own home location, thereby making them more resilient to local demand shocks.⁶⁶

A regulation that severely hinders data-driven advertising would not only impact the largest companies in the marketplace, but more ominously also would impact myriad other small, medium, and large companies as well as individuals employed by those companies at a time of significant economic uncertainty. The power of data-driven advertising should be harnessed to provide benefits to consumers and support a healthy economy, instead of limiting or impairing it. The Agency should strike a balance between fostering continued economic development and providing robust privacy protections for Californians through the CPRA regulations. The CPPA should keep the benefits of data-driven advertising in mind as it updates the proposed regulations implementing the CPRA.

⁶⁴ Digital Advertising Alliance, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located [here](#).

⁶⁵ Deloitte, *Dynamic Markets: Unlocking small business innovation and growth through the rise of the personalized economy* at 2 (May 2021).

⁶⁶ *Id.* at 23.

* * *

Thank you for the opportunity to submit comments on the proposed regulations to implement the CPRA. Please do not hesitate to contact us with any questions regarding this submission.

From: **Edwin Portugal** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Matt Kownacki** [REDACTED]; **Danielle Arlowe**
Subject: CPPA Public Comment - AFSA Letter on Proposed Rules
Date: 23.08.2022 20:21:51 (+02:00)
Attachments: AFSA comment letter - CA CPPA 2022 privacy rulemaking.pdf (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

Thank you for the opportunity to comment on the California Privacy Protection Agency's proposed privacy rules. Attached are comments from the American Financial Services Association on the Agency's proposed rules.

Please let us know if you have any questions.

Thank You,
Edwin Portugal



Edwin Portugal
Manager, State Policy & Regulatory Affairs

[REDACTED]
[@AFSA_DC](#) | [Linkedin](#) | [@AFSA_SGA](#)

August 23, 2022

California Privacy Protection Agency
Attn: Brian Soubllet
2101 Arena Blvd.
Sacramento, CA 95834

Re: Comments on proposed rulemaking implementing the California Privacy Rights Act of 2020

Dear Mr. Soubllet:

On behalf of the American Financial Services Association (“AFSA”),¹ thank you for the opportunity to provide comments on the California Privacy Protection Agency’s (“Agency”) July 8 proposed rulemaking to implement the California Privacy Rights Act of 2020 (CPRA). AFSA members share the state’s goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access. We appreciate the Agency’s consideration of our previous comments and look forward to further engagement throughout the rulemaking process.

Enforcement Delay

The CPRA requires that finalized regulations be completed by July 1, 2022 to provide businesses with enough time to comply before January 1, 2023, when the CPRA becomes operative, and before enforcement begins six months later, on July 1, 2023. However, the Agency has indicated that the regulations will not be finalized until the third or even fourth quarter of 2022, leaving businesses with very little time, if any, to comply. While we understand this rulemaking process is complex and appreciate the Agency’s work and consideration of comments throughout the process, we believe a delayed effective date and enforcement date are necessary. The proposed rules would require numerous updates to existing operational systems, including changes to contracts with third-party service providers, website changes and training staff. Therefore, we request that the final rules include a delayed effective date of at least January 1, 2024, and a delayed enforcement date of at least July 1, 2024, which will allow affected financial institutions adequate time to implement the required changes.

§ 7002. Restrictions on the Collection and Use of Personal Information.

Under the proposed regulations, businesses have to obtain the consumer’s *explicit consent* before collecting, using, retaining, and/or sharing the consumer’s personal information for purposes unrelated to, or incompatible with, the purposes for which the personal information was originally collected or processed. The CPRA requires businesses to give consumers notice at the point of personal information collection regarding the categories of information to be collected and the purposes for which this

¹ Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

information will be used. In addition, a supplementary notice to consumers is required if any additional categories of personal information will be collected, or if the collected personal information will be used for purposes incompatible with the ones initially disclosed. The requirement for explicit consent, in addition to the other notices and requirements, will make it more difficult for businesses to evolve and improve their products and services over time. Businesses should not have to obtain an additional consent from the consumer if they fully disclosed all of the potential purposes for which the information may be used, retained or shared (so long as they are not incompatible with the purposes for which the information was originally collected). Developing and marketing new products or improving and marketing existing products would not be feasible.

§ 7004. Consumer Consent.

Section 7004(b) states that activities that do not comply with specific guidelines proposed in the rules constitutes a “dark pattern” and that businesses using “dark patterns” should not be considered to have obtained consumer consent. Section 7004(c) further states that a “user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent.” As written, the draft regulations subject businesses to strict liability regarding the development and implementation of their user interfaces. As a consequence, the Agency or Attorney General could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that may accidentally cause a substantial subversion or impairment of a user’s autonomy, decisionmaking, or choice. It is common for businesses of all sizes to experience problems with their websites, online user interfaces, and mobile applications. Moreover, these problems can occur without the business’s negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminal actors can alter or disrupt a business’s online presence despite the business’s use of state-of-the-art security measures. A business should not be punished for something it did not intend or cause nor could have prevented. We request that the agency drop the strict liability in exchange for a more-measured approach that considers the business’s intent, knowledge, and other relevant factors, such as information security practices. Alternatively, if the regulations retain strict liability, we request that they also establish a safe harbor provision that protects businesses from liability for violations that could not have been prevented or expected.

§ 7011. Privacy Policy.

Section 7011(e) requires a business’s privacy policy to include content not mentioned in the statute. For example, Section 7011(e)(1) requires “a comprehensive description of the business’s online and offline practices regarding the collection, use, sale, sharing, and retention of personal information.” However, the statute does not mention any requirement that the privacy policy contain a “comprehensive description” of a business’s “online and offline practices.” We request that the regulations align with the statute and provide additional guidance or clarity, not create unanticipated requirements with undefined terms such as “comprehensive description.”

§ 7012. Notice at Collection of Personal Information.

Section 7012(e)(4) requires the notice at collection to include the “length of time the business intends to retain each category of personal information,” or if that is impossible, the “criteria used to determine the period of time” the personal information will be retained. Prescriptive data retention notice requirements

are difficult to comply with because of the various and numerous factors that could come into play, such as duration of the relationship with the consumer, duration of the transaction, legal requirements, or in anticipation of defending against legal claims or litigation. We respectfully request that this provision be stricken or amended to allow greater flexibility.

Section 7012(e)(6) requires a business that allows third parties to control the collection of personal information to include in the notice at collection, “the names of all third parties; or, in the alternative, information about the third parties’ business practices.” The statute requires only disclosure of “categories” of third parties, never names or business practices, in the privacy policy, the notice at collection, and in response to the right to know/access. We ask that the agency modify this section to track with the statute requiring categories of third parties, not names or business practices.

Section 7012(f) would require that the notice at collection, if provided online, link to a privacy policy and that the link would take the consumer directly to the applicable section of the privacy policy. This is extremely burdensome and technologically challenging to accomplish. We would suggest, instead, requiring a privacy policy to have sections outlined at the beginning of the privacy policy which enable the consumer to click on the section and be taken to that section of the privacy policy. This flexibility would provide consumers with easy access to the information but would be much more technologically feasible.

Under Section 7012(g)(2), if a business allows third parties (i.e., not service providers or contractors) to control the collection of personal information, the consumer needs to be informed of these third parties’ names or business practices in the privacy notice that they receive at the time of collection of their personal information. Similar to the issue with Section 7012(e)(6) outlined above, the requirement for a business to name or describe the third parties with which it shares personal information would require privacy notices to contain long lists of company names or descriptions that are prone to becoming outdated over time. A lengthy notice prone to including outdated information could end up being so voluminous as to become meaningless to consumers. Accordingly, we request this requirement be removed from the regulations.

§ 7013. Opt-Out Notice.

Section 7013(e) requires a business that “sells or shares” person information provide a notice of right to opt-out of “sale/sharing.” Under current statute and Attorney General regulations, a business that does not “sell” personal information is not required to post a “Do Not Sell My Personal Information” link. Under the proposed draft regulations, if a business “shares” but does not “sell” personal information, the regulations require a business to post a “Do Not Sell or Share My Personal Information” link or the alternative link. If a business “shares” but does not “sell,” or vice versa, the business should be able to post the relevant link and not both links. For example, the business that does not “sell” but “shares” should be permitted to post a “Do Not Share My Personal Information” link without the inclusion of “sell.”

§ 7022. Requests to Delete. & § 7023. Requests to Correct.

Section 7022(b)(1) requires businesses to delete a consumer’s personal information from its existing systems with exceptions for “archived or back-up systems,” indicating that requests to delete do not

trigger a requirement to delete personal information on archived or back-up systems. However, Section 7022(d) states that a business that stores any personal information on archived or back-up systems “may delay compliance with the consumer’s request” until the archived or back-up system is “restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.” We respectfully request that the Agency clarify if a business is never required to delete personal information stored on archived or back-up systems (as long as it says on such archived or back-up systems), or a business has a requirement to delete personal information on archived or stored systems; however, that requirements are not triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose. Additionally, we would like clarification if the definition of “access” includes de minimis, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned.

Section 7022(f)(1) and Section 7022(f)(2) would require a covered entity to provide a factual, detailed explanation that gives the consumer a meaningful understanding of the disproportionate effort that prevented compliance with a request to delete or correct. The reasons for disproportionality are complex, and some would require a comprehensive understanding of the business’ technical internal processing platform that the consumer does not have. Without this understanding, a detailed explanation would likely confuse, rather than inform, the consumer’s understanding of the process, and the requirement to provide a detailed explanation should be stricken from the rules.

Similarly, the CPRA provides numerous reasons that allow businesses to decline a request to delete or correct. For example, for a consumer request to delete, a financial institution may be able to retain data due to the Gramm Leach Bliley Act (GLBA) exemption, if the account is still open, if the legal records retention period has not expired, etc. Each of these would need to be captured for each individual request and detailed further in the individual consumer response. The complex response required for such a response would be burdensome for the company and may overwhelm or confuse a consumer. Additional complexity exists for other types of requests beyond this specific example. Accordingly, we respectfully request that the requirement to provide a detailed explanation be removed from the rules.

§ 7024. Requests to Know.

Under the CPRA, when a business receives a verifiable consumer request to access their personal information, the disclosed information should cover the 12 months preceding the request. The CPRA allows the regulations to extend this 12-month look-back period unless doing so proves impossible or would involve disproportionate effort on behalf of the business. Accordingly, the proposed regulations impose a look-back period back to January 1, 2022, and also extend the scope of requests to personal information in the hands of the business’s service providers and contractors. This broadening of personal information that is subject to consumer requests will make honoring requests more burdensome for businesses. The regulations should not broaden the personal information that is subject to consumer requests, if it is not explicitly stated in the CPRA.

§ 7025. Opt-Out Preference Signals.

The CPRA provides businesses with different options regarding how businesses can enable consumers to exercise their opt-out rights, for instance by providing opt-out links, or by honoring opt-out preference signals received from consumers' devices or applications. However, the proposed regulations require that opt-out preference signals need to be complied with regardless of whether a business has chosen to provide the opt-out links. This requirement has no basis in the CPRA and exceeds the Agency's authority. Taking away a business's option between providing opt-out links and honoring preference signals is overly burdensome, and the regulation should retain a business's choice between providing opt-out links and honoring preference signals, as provided by the CPRA.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

In a number of sections, the regulations contravene and narrow the scope of the statutory language. This effectively disregards Section 1798.121(a)-(b) of the statute, which permit a business to use a consumer's sensitive personal information for uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," even after receipt of a consumer's request to limit. While the regulations attempt to define permissible uses of Sensitive Personal Information in Section 7027(l), the seven use cases listed do not encompass all those uses of Sensitive Personal Information that may be "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

We believe that the rules' narrow scope has significant adverse effect. As an example, in Section 7014(h), the Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of Sensitive Personal Information collected at a time when a business did not have a notice of right to limit posted. As written, since a notice of right to limit is not required until January 1, 2023, any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l). Similarly, in Section 7027(g)(1), the Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose Sensitive Personal Information for any purpose other than the seven purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services." We believe that these inconsistencies are extremely problematic for constructing a compliance program. Furthermore, the seven use cases identified in 7027(l) do not contemplate a use of Sensitive Personal Information to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information. Accordingly, we respectfully request that the Agency reconsider such narrowly defined uses or add an additional section allowing "any other acts or practices that may be necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

CPRA Section 1798.121(d) states that the requirements in the CPRA related to limiting usage of sensitive personal information and providing a usage limit link don't apply if sensitive personal information is collected and processed without the "purpose of inferring characteristics about a consumer." The proposed regulations do not include this exception. Instead, the regulations may be subjecting all businesses to the CPRA's usage limitation and link requirements, including those who do

not use sensitive personal information for the purpose of inferring characteristics. The regulations should be revised to reflect the exception under Section 1798.121(d), and be revised to provide guidance and examples of what it means to use sensitive personal information to infer and not infer characteristics about a consumer.

§ 7050. Service Providers and Contractors.

The proposed regulations are very prescriptive about the exact provisions that need to be in any contract with a third party that is considered a service provider. These burdensome provisions will make compliance exceptionally difficult, and we believe additional flexibility would provide the desired protections while easing the compliance burden.

§ 7051 Contract Requirements for Service Providers and Contractors. & § 7053 Contract Requirements for Third Parties.

The proposed regulations limit the CPRA's safe harbor for businesses based on their due diligence of their service providers and other parties. Under the proposed regulations, if a business fails to enforce contractual terms and fails to audit or test its service providers', contractors', or third parties' systems, the business might not be able to claim that it did not have reason to believe that its service providers, contractors, or third parties intended to use the personal information in violation of the CPRA. This erodes the safe harbor that would otherwise protect a business whose service provider fails to comply with the CPRA despite its contractual and statutory duties to do so. The limit to the CPRA's safe harbor for businesses based on their due diligence of their service providers and other parties should be removed from the regulations.

The proposed regulations require similar contractual provisions in agreements between businesses and their service providers or contractors as the required contractual provisions between businesses and other third parties. Since the nature of a relationship between a business and its processor is fundamentally different from its relationship with another controller, having the same contractual provisions, such as purpose limitations and oversight provisions, in both kinds of agreements is unlikely to accurately reflect the true relationship and allocation of responsibilities of the two parties. Additionally, new contractual requirements put additional burdens on businesses that need to negotiate and update potentially hundreds or thousands of agreements. This is time consuming and costly to the business and ultimately the consumer if reflected in the price of products and services. The regulations should automatically bind the required contractual provisions to service providers, contractors and third parties. If the contract includes a compliance with laws representation, the relevant provision of the CPRA would be included by reference into the contract. This is more efficient and will considerably reduce the cost to update contracts.

§ 7063. Authorized Agents.

The requirements in Section 7063(b) should remain unmodified, as an opportunity for fraud is created by allowing a consumer to authorize an agent to manage their personal information based on a simple signature without a requirement for the agent to be registered or for the consumer to provide a power of attorney or a notarized signature.

Extension of Employee and B2B Exemption

The California Privacy Rights (CPRA) extends the CCPA's partial exemption of employee and business contact data until January 1, 2023. The expiration of the exemptions will leave employees, job applicants, employers and individuals serving other businesses in a service provider context confused regarding the interplay between the CPRA and employment laws because most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context. We recommend that in future rulemakings the Agency consider making the exemptions permanent or extend them to at least January 1, 2024, to allow for additional time to comply, if the legislature fails to take steps to extend them.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at [REDACTED] or [REDACTED]

Sincerely,
[REDACTED]

Matthew Kownacki
Director, State Research and Policy
American Financial Services Association

From: **Joanne Furtsch** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 13:23:26 (+02:00)
Attachments: CCPA Regulation Comments_FINAL.pdf (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attn: Brain Soublet

Please find TrustArc's comments regarding the proposed updates to the CCPA Regulation attached. Contact me if you have any questions.

Best -
Joanne Furtsch

--

Joanne B. Furtsch

Director, Privacy Intelligence Development / CIPP/US/C, CIPT, FIP

M: [REDACTED] | [REDACTED]

CONFIDENTIALITY NOTICE: This email including any attachments, may contain information that is confidential. Any unauthorized disclosure, copying or use of this email is prohibited. If you are not the intended recipient, please notify us by reply email or telephone call and permanently delete this email and any copies immediately.

August 23, 2022

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834
Attn: Brain Soublet

By Email Submission to: regulations@coppa.ca.gov

RE: TrustArc's CCPA Public Comment

TrustArc Inc ("TrustArc") appreciates the opportunity to provide comments on the text of the proposed California Consumer Privacy Act Regulations. TrustArc knows well the challenges consumers face in protecting their personal information and businesses encounter when implementing new laws and regulations. TrustArc agrees that clear guidelines for businesses to implement the law's requirements are necessary to ensure consumers are able to easily and effectively manage their rights under the California Consumer Privacy Act.

Our concerns center around the cost and effort to implement that may overshadow consumer rights. There is an opportunity to clarify the requirements in a way that enables businesses, and their service providers and contractors to comply.

We want to emphasize the following:

- Rules need to be clarified around how a business needs to obtain new consent when there is a conflict between the consumer's established preference and browser signal setting.
- The mechanisms businesses must implement to communicate whether a consumer's preference signal is being honored need clear requirements.
- The new requirements to manage third party service providers and contractors open the door for contractual abuse if not specifically addressed, especially for small businesses that do not have leverage to change or update service agreements.

Our detailed comments are provided below. For any questions regarding this submission, please contact Joanne Furtsch, Director, Privacy Intelligence Development, at [REDACTED]

I. OPT-OUT SIGNALS

A. § 7025. Opt-out Preference Signals May Increase Consumer Consent Fatigue.

Issue

Consumers are constantly inundated now with making choices about the use of trackers to the point that they accept (or decline) everything without understanding the effect on their rights. The following implementation may create an endless loop.

Requirement: c(3)

(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display in a conspicuous manner the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

Example: c(7)(B)

(B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.

Problem

TrustArc believes there may be an endless loop with how the requirement in c(3) may be implemented based on the example described in c(7)(B).

Each time the consumer ("Noelle") visits the website with her opt-out preference signal on and is not yet logged in, the opt-out signal must be honored. If she logs in, and her preferences conflict with the opt-out signal, she has to confirm consent to the sale/sharing of her personal information. This will happen each time she visits the site because the site does not recognize her until she logs in.

If she logs out of the site and then comes back (opt-out preference signal is on), the signal is honored, she logs back in, new confirmation of consent is required because there is a conflict between her preference and the signal. She is considered opted-out until she consents again.

This will happen each time she logs out and revisits the site, creating an endless cycle of the site having to obtain new consent and a poor user experience each time she visits the site.

Recommendation

A clarification needs to be added explaining that once a consumer has consented to the sale/sharing of their personal information and the business has logged receiving the consumer's consent while their preference signal was on, the signal can be subsequently ignored when the consumer logs back in again and the site recognizes that the consumer as having consented to the sale/sharing of their personal information. Consent then does not need to be collected each time the consumer logs back in.

If the consumer does not log in, and is not recognized by the site, then the preference signal must be honored for that device until the consumer logs in and is recognized by the site.

B. § 7025. Opt-Out Preference Signals Need Clear Implementation Requirements.

Issue

Opt-out preference signal being honored indicator as described in c(6) is unclear about what exactly is required.

Requirement: c(6)

(6) The business should display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

Problem

It is unclear what the "honored" indicator needs to look like and how businesses should go about implementing this requirement. For example, if a business implements a toggle or radio button as described in c(6), what effect clicking the toggle or radio button is supposed to have is unknown.

Recommendation

The proposed regulation should outline clear requirements for implementing the opt-out preference signal honored indicator. Requirements should address where on the website does the indicator need to appear and how prominent does it need to be in relation to other items on the website. If the toggle or radio button is implemented, explain what the toggle is expected to do and the types of actions a consumer could take.

Consider allowing the use of an icon, something similar to the DAA Ad Choices icon, that is easily recognizable, does not take up much real estate on the site, and is easily actionable by consumers.

II. CONTRACTUAL ISSUES FOR SERVICE PROVIDERS AND CONTRACTORS

A. Article 4 § 7051 Contract Requirements for Service Providers and Contractors.

Issue

Potential for contractual requirements that lead to ineffective and non-compliant business operations.

Requirement: (a)(6)

(a) The contract required by the CCPA for service providers and contractors shall

*(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including providing the **same** level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.*

Problem

The problem is not in the intent, but in how the wording will be implemented. The word “same” where bolded in (a)(6) of Article 4 § 7051 can create a level of contractual complexity that can make it nearly impossible for any business to meet the requirements, especially a small business or a contractor who is typically an individual.

In particular, a service provider’s customers will each tend to add specific privacy and security controls rather than requiring “reasonable” procedures and practices - emphasizing the “same” rather than the “same level.” The varied specificity will create an impossible compliance regime for service providers. Whereas a service provider can negotiate their own controls, they may be required to push down the “same” controls to their subcontractors; thus, compounding the conflicting requirements.

Thus, the problem is in the interpretation and implementation. It is not possible for a service provider to have the **same** privacy protection as required by all of its customers, although the **same level** is possible.

Recommendation:

1. Replace the word “same” with “appropriate” to read “...including providing appropriate levels of privacy protections as required by all its customers...”
2. Add a requirement for the service providers to meet the CCPA level of protection imposed and make it clear that meeting the CCPA standards is sufficient.

This will align California’s requirements with other U.S. state laws and federal laws such as HIPAA (the Health Insurance Portability and Accountability Act of 1996, along with its subsequent amendments, “HIPAA”) as noted in the two examples below.

Example 1:

Under the Colorado Privacy Act CRS 6-1-1305(4)¹, processors are required to implement “...appropriate technical and organizational measures to ensure a level of security appropriate to the risk...”.

(4) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.

Example 2:

The HIPAA Security Rule 45 CFR § 164.308² - Administrative safeguards. (b)(1) and (b)(2) use the phrase “...obtains satisfactory assurance that they will appropriately safeguard the information...”

(b)
(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

B. Article 4 § 7051 Contract Requirements for Service Providers and Contractors**Issue**

Clarification desired for self reviews or third-party review to meet the requirement.

Requirement: (a)(7)

(a) The contract required by the CCPA for service providers and contractors shall

(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.

¹ Colorado Privacy Act [CRS 6-1-1305\(4\)](#)

² [HIPAA Security Rule 45 CFR § 164.30 \(b\)\(1\) and \(b\)\(2\)](#)

Problem

It is not clear whether the draft regulation allows service providers to use third party audits or certifications as a means to fulfill the audit requirement in Article 4 § 7051(a)(7) and enable businesses to recognize those as such.

Both the Colorado Privacy Act³ and Virginia Consumer Data Protection Act⁴ allow for processors to use a qualified and independent third party to conduct an audit to ensure that the processor is meeting its obligations.

Recommendation:

Include independent third party reviews, and specify certifications and validations as a means to satisfy the audit requirement by adding the words “internal or third party” and “certifications and validations” to the last sentence to have it read as follows:

Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular internal or third party assessments, audits, certifications and validations, or other technical and operational testing at least once every 12 months.

This will align the regulation with other U.S. state consumer privacy laws that recognize independent third party reviews as a means to demonstrate compliance.

C. Article 4 § 7051 Contract Requirements for Service Providers and Contractors**Issue**

Disproportionate impact on small businesses if audits or tests are required as a defense.

Requirement: (e)

(e) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider’s or contractor’s systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Problem

If a business does not exercise the right to audit its service providers, it puts them at a disadvantage. For example, small businesses use a variety of cloud services to manage their business and the personal information that is collected. Large service providers such as Google, Oracle, and Salesforce have services that cater to small businesses. Small businesses are not able to impose a right to audit on these organizations. If a large service provider is using personal information in violation of CCPA, a small business

³ Colorado Privacy Act [CRS 6-1-1305 - Responsibility according to role - Audits](#)

⁴ Virginia Consumer Data Protection Act [§ 59.1-575. B. Responsibility according to role: controller and processor. - Contracts](#)

will be unable to effectively defend itself if it is unable to “audit” or “test the . . . systems” of the service provider.

If the small business is a service provider, it is costly for them to submit to such audits making it harder for them to compete against larger competitors.

Recommendation

Allow business to rely on public third party audit results (e.g., SOC 2 reports) or third party certifications or validations conducted by an independent and qualified third party. As noted above, both the Colorado Privacy Act and Virginia Data Protection Act allow for the recognition of third party audits, certifications, and validations as a means to ensure processors are meeting their obligations under these laws.

Some large service providers like Salesforce already have areas of their website⁵ dedicated to building trust and demonstrating compliance listing out the third party audits and certifications they undergo. Validation of these certifications can be easily checked by businesses and consumers.

D. § 7053. Contract Requirements for Third Parties.

Issue

Infeasible requirement for current state of technology.

Requirement: (b)

(b) A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party’s own purposes, shall contractually require the third party to check for and comply with a consumer’s opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.

Issue

This requirement is difficult for any business with third party contracts to manage. It places administrative burdens on businesses requiring processes and mechanisms by which to communicate the consumer’s consent. Implementation will be difficult to enforce due to a lack of consistency across customers (e.g., a third party complying with various customer requirements) and current state of technology and interoperability.

Recommendation

Table this requirement until uniform opt-out global privacy control is adopted.

Conclusion

Thank you for your time and consideration. We look forward to enhancements and further clarification as noted above. For any questions regarding this submission, please contact Joanne Furtsch, Director, Privacy Intelligence Development, at [REDACTED].

⁵ https://compliance.salesforce.com/en?_ga=2.131851719.912381987.1659482552-1570373810.1659482552

From: **Irene Ly** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Jolina Cuaresma** [REDACTED]
Subject: CPPA Public Comment - Common Sense Media
Date: 23.08.2022 16:43:42 (+02:00)
Attachments: CSM Comments on CPPA Rulemaking Aug. 2022.pdf (4 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

Please see attached for Common Sense Media's written comments on the Agency's proposed regulations. Thank you for the Agency's time and consideration of these comments.

Best,

Irene Ly

Policy Counsel | Common Sense

p: [REDACTED] e: [REDACTED]



August 23, 2022

California Privacy Protection Agency
c/o Brian Soublet
2401 Arenal Blvd
Sacramento, CA 95834
via email at regulations@coppa.ca.gov

Dear Mr. Soublet:

Common Sense Media (Common Sense) submits these comments on the California Privacy Protection Agency's (Agency) proposed regulations that, if finalized as proposed, would implement the California Privacy Rights Act (CPRA). Common Sense is the nation's leading independent nonprofit organization dedicated to helping kids and families thrive in an increasingly digital world. We empower parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in children's lives.

While the CPRA strengthened the California Consumer Privacy Act (CCPA), even stronger protections are needed for kids and teens. Under existing law, parents do not know whether their children's privacy is protected. For kids and teens under 16, they have rights only when a firm has "actual knowledge" of their age. In other words, even when the largest social media firms have a strong inference of their users' age—based on millions of data points about them—these firms can continue to sell and share children's personal information as long as they avoid obtaining direct information about age. While our comments below speak directly to the proposed regulations, we urge the Agency to support legislation that grants kids and teens the protections they need.

Common Sense appreciates the opportunity to provide the Agency with the following comments, which are limited to those proposed regulations pertaining to consumers under 16.

Comments to §§ 7070 and 7071.

1. *We recommend the Agency define the term “actual knowledge” to include the meaning of “willfully disregard.”*

Section 1798.120(c) of the CCPA, as amended by the CPRA (Act) mandates certain requirements when a business has “actual knowledge” that a consumer is under 16 years of age. It also provides that “[a] business that willfully disregards the consumer’s age shall be deemed to have had actual knowledge of the consumer’s age.” The Agency’s proposed regulations sections 7070 and 7071, however, make no reference to the “willfully disregard” language.

The Agency’s regulations should make clear that if a business purposefully, deliberately, or intentionally disregards a consumer’s age, it would be deemed to have actual knowledge.

To make the Agency’s proposed regulations consistent with the California Consumer Privacy Act (CCPA), as amended by the CPRA, we offer the following definition for consideration:

“‘Actual knowledge’ means actual awareness, understanding, or recognition of a fact. The term also includes willful, purposeful, deliberate, or intentional disregard of a fact.”

2. *We recommend that the Agency make clear the responsibilities of a business once it has actual knowledge that a consumer is under 16 years of age.*

Section 1798.120(c) of the Act implies that a business may continue to sell or share a consumer’s personal information until it has actual knowledge that the consumer is under the age of 16. It also implies that the business must stop selling or sharing such information until it obtains consent. The Agency should make these two implications explicit in its proposed regulations.

We offer the following for consideration:

“Once a business has actual knowledge that a consumer is under 16, it must immediately stop selling or sharing personal information about the consumer. A business cannot resume selling or sharing personal information unless it has obtained consent from: (1) the parent or guardian of consumers under the age of 13; or (2) consumers if they are between the age of 13 and 16.”

3. *We recommend the Agency correct the definition of “COPPA” under section 7000(g) because the term is used in its proposed regulations sections 7070 and 7071.*

We offer the following edits for consideration:

“‘COPPA’ means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506~~08~~ and 16 Code of Federal Regulations part 312.5.”

First, we recommend striking 6508 and replacing it with 6506 because the Children’s Online Privacy Protection Act is codified at 15 U.S.C. sections 6501 to 6506 (i.e., sections 6507 and 6508 do not exist). Next, section 7001(g) should define “COPPA” to include all regulations promulgated under the federal statute. Under the existing section 7001(g), “COPPA” is defined to mean the federal statute in its entirety and only a single regulation, despite multiple regulations having been promulgated. We recommend the Agency resolve this discrepancy. Finally, we recommend that the Agency define “COPPA” to include language that would account for any amendments made to the federal statute, and any amended or new regulations promulgated thereunder.

Comments to § 7070.

1. We recommend the Agency establish a specific time by when a business must inform parents or guardians of consumers under the age of 13 of their right to opt out of the sale or sharing of their personal information

Under section 7070(b), a business must inform the parent or guardian of consumers under 13 that they may opt-out of the sale or sharing of personal information on behalf of their child “when” a business receives consent to the sale or sharing of personal information. We believe that “when” suggests that the parent or guardian must receive this information at the same time or close in time to the business’s receipt of parental consent.

To make clear a business’ responsibilities under this section, we offer the proposed edits for consideration.

~~“When a business receives an affirmative authorization~~ **Within 48 hours of receiving consent to the sale or sharing of personal information** pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).”

Comments to § 7071.

1. We recommend the Agency amend the title of proposed regulation section 7071. Section 7071 is entitled “Consumers 13 to 15 Years of Age.” Yet, subsections (a) and (b) reference “consumers 13 years of age and less than 16 years of age.”

We recommend the Agency retitle this section to “Consumers between 13 and 16 Years of Age” to make clear that the section applies to teens until the day that they turn 16 years of age.

2. *We recommend the Agency establish a specific timeframe by when a business must inform consumers between the age of 13 and 16 of their right to opt out of the sale or sharing of their personal information.*

Under section 7071(b), when a business receives an opt-in request from consumers between the age of 13 and 16, the business must inform them of their right to opt-out “at a later date.” We believe that it is critical for these consumers – who are still minors – to know their right to opt-out in a timely fashion. Without a set timeframe, the Agency would implicitly allow businesses to indefinitely delay providing this information.

Conclusion

Common Sense appreciates the Agency’s work on these proposed regulations to implement the CPRA, and urges the Agency to take the steps recommended in these comments to revise and provide further clarity to the proposed regulations pertaining to consumers under 16. Thank you for your consideration of these comments.

Respectfully submitted,

Jolina Cuaresma
Senior Counsel, Privacy and Technology Policy

Irene Ly
Policy Counsel

From: **Greaves, Fielding** [REDACTED]
 To: **Regulations** <Regulations@cpga.ca.gov>
Moira Topp [REDACTED]; **Abrahamson, Reed C.F.**
 CC: [REDACTED]; **Blenkinsop, Peter**
 [REDACTED]; **Kuzma, Clare M.**
 [REDACTED]; **Greaves, Fielding** [REDACTED]
 Subject: CPPA Public Comment - Biocom California & IPMPC
 Date: 23.08.2022 20:56:55 (+02:00)
 Attachments: CPRA July 8 Proposed Draft Regulations - Biocom California and IPMPC Comments 8-23-22.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please accept the attached comments for the NPR published July 8, 2022 for CPPA regulations.

Please let me know if you have any questions.



Fielding Greaves

Sr. Director, State Government Affairs

San Diego | Los Angeles | Bay Area | Sacramento | Washington, D.C. | Tokyo

1111 L Street | Sacramento, CA 95814

[REDACTED] | [REDACTED] | www.biocom.org



Support Children & Families in Ukraine
 Donate Now

Biocom California IN SUPPORT OF **unicef** USA



August 23, 2022

California Privacy Protection Agency
 Attn: Brian Soubllet
 2101 Arena Blvd.
 Sacramento, CA 95834

Via email to regulations@cpha.ca.gov

Subject: Public Comment on Notice of Proposed Rulemaking (July 8, 2022)

Dear California Privacy Protection Agency:

Biocom California and the International Pharmaceutical & Medical Device Privacy Consortium (“IPMPC”) welcome the opportunity to provide comments on the Agency’s proposed regulations implementing the Consumer Privacy Rights Act of 2020 (“CPRA”) and revising the regulations issued previously under the California Consumer Privacy Act of 2018 (“CCPA”).

Biocom California is the state’s premier life sciences organization representing over 1,700 member companies throughout California. Biocom California is a leading voice in the advocacy efforts of the California life science community whose members include biotechnology, pharmaceutical, medical device, genomics and diagnostics companies of all sizes, research universities and institutes, clinical research organizations, investors and service providers.¹

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical and medical-device manufacturers. The IPMPC is the leading voice in the global pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.²

Our specific comments are below, but we would like to make a few general observations. First, we thank the Agency for including examples illustrating key concepts and providing interpretive insight. These examples are critical to structuring effective privacy compliance programs. Second, we would urge the Agency to add even more examples to the draft regulations. Many of the concepts discussed would benefit from a practical, real-world illustration showing how the Agency views the matter at hand.

¹ More information about Biocom California is available at <https://www.biocom.org>. These comments reflect the position of the Biocom California as an organization and should not be construed as the positions of any individual member.

² More information about the IPMPC is available at <https://www.ipmpc.org>. These comments reflect the position of the IPMPC as an organization and should not be construed as the positions of any individual member.

Finally, we ask the Agency to develop and release sample notices and data subject responses. We appreciate that the CPRA and the Agency have urged businesses to present information to consumers in clear and understandable ways. However, the CPRA and draft regulations also require that this information be comprehensive and detailed. As science-based organizations, we are mindful that detailed and comprehensive descriptions may not always be simple or easy to understand. We work continuously to ensure that our communications can be understood by patients and caregivers, but we would appreciate further guidance from the Agency about its expectations.

§7002(b)(2) Restrictions on the Collection and Use of Personal Information, example involving cloud storage services for consumers.

We request that this example be clarified to avoid implying that deletion of consumer data is required in all cases once a consumer ends its business relationship with a company.

Other sections of the CPRA (including the exceptions to the consumer’s right to deletion) acknowledge that data may be retained for permissible purposes or in archive or back-up forms. We encourage the Agency to make it clear that the general requirement that “collection, use, retention or sharing of data be necessary and proportionate to the purposes” for which the information was originally collected does not override more specific language found elsewhere in the CPRA and the draft regulations about specific situations in which data may be permissibly used and retained.

§ 7014(a) Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link.

This provision states that the “purpose of the ‘Limit the Use of my Sensitive Personal Information’ link is to immediately effectuate the consumer’s right to limit, or in the alternative, direct the consumer to the notice of the right to limit.” (emphasis added). We believe the word “immediately” could lead to confusion – elsewhere, the regulations permit a business to implement a request to limit the use of a consumer’s sensitive information “as soon as feasibly possible,” but always within 15 days. See §7027(g)(1). We encourage the Agency to remove the word “immediately” in §7014(a) to avoid contradiction.

§ 7022(c)(4). Requests to Delete, notification to other parties.

We request that this language be clarified. The use of the word “may” creates ambiguity: “Notifying any other service providers, contractors, or third parties that may have accessed personal information” We assume the Agency wishes to require notification to anyone who did access personal information, not to anyone who simply could have accessed personal information (including those that, in fact, did not). Omitting “may have” in the quoted language would leave a clearer regulatory requirement.

§ 7022(f)(1). Requests to Delete, denials by a business.

We ask that the Agency provide examples of the kind of information that would satisfy the requirement for a “detailed explanation” of the basis for denial. The regulations currently require that the basis be “described.” The change from “described” to “detailed explanation” suggests the Agency anticipates businesses will provide the consumer with more information than they had previously. But the substantive requirement to identify a conflict with federal or state law or an exemption to the CCPA has not changed, so it is not clear what other information the Agency wants businesses to provide.

§ 7025(b). Opt-Out Preference Signals, requirements for valid requests.

The Agency should identify and provide technical examples of formats that are “commonly used and recognized by businesses.” We do not believe that there is a common and recognizable format for opt-out signals in the market at this time. We suggest that the Agency identify a particular technology or standard format and provide for an implementation period before any of the related regulations come into effect. This would allow technologists and businesses to develop compliance tools that work as the Agency intends. Regulatory endorsement of a particular approach would speed adoption and improve compliance.

§ 7025(e). Opt-Out Preference Signals, processing choices.

The Agency’s statement that 1798.135(b) “does not give the business a choice between posting the above-referenced links or honoring opt-out preference signals” appears contrary to the plain language on 1798.135(b) and other provisions of the CPRA. 1798.135 clearly sets up two approaches for facilitating opt-out requests – a business can either post the links or honor consumer opt-out “signals.” Doing both, as the Agency suggests, is not required. 1798.135(b)(3) makes it very clear that “a business may elect whether to comply with subdivision (a) [posting links] or (b) [honoring opt-out signals].”

This clear statement is further supported by the text of 1798.135(b)(1), which states that a business is not required to post Do Not Sell or Share links “if the business allows” (emphasis added) consumers to opt-out via an “opt-out preference signal.” The use of “if” and “allow” clearly indicate that honoring opt-out preference signals is not required under the CPRA. The use of the word “allows” is repeated in 1798.135(b)(2). In addition, the delegation of rule-making authority to the Agency in 1798.185(a)(20) empowers the Agency to make regulations that govern how “a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal” (emphasis added). All of this language indicates that businesses have a choice between posting links or honoring opt-out signals.

The Agency’s proposed approach requires businesses to allow consumers to opt-out via a preference signal. This is inconsistent with the text of the CPRA, which clearly gives businesses a choice between posting links or responding to signals. The Agency suggests that the choice is instead between “frictionless” and “non-frictionless” responses to opt-out signals. However, the term “frictionless” does not appear in the CPRA. The CPRA does not contemplate two different kinds of responses to opt-out signals – it just describes two options for receiving such signals.

§ 7027(e). Requests to Limit Use and Disclosure of Sensitive Personal Information, requests to limit.

We ask that the Agency treat requests to limit use of sensitive personal information according to the same time periods as other consumer rights and provide clear guidelines for how businesses should collect additional information. Admittedly, the CPRA does not specifically require verification of the identity of a consumer who seeks to limit the use of their sensitive personal information. However, as the Agency acknowledges, it may be necessary for a company to ask for additional information in order to identify the right consumer. A limitation on the use of a consumer’s sensitive personal information has the potential for negative consequences for the consumer (especially if misapplied), and businesses should be allowed time to make sure the right person is impacted and requested the limitation at issue.

Especially in the healthcare context, it may take courage for a consumer to share sensitive information about their racial identity, sexual orientation, and health condition. Mistakenly terminating the use of such information could leave a consumer upset. Companies should be provided with time and a process to make sure limitations are applied to the right person.

§ 7027(l)(7). Requests to Limit Use and Disclosure of Sensitive Personal Information, allowable uses and disclosures not requiring notice of a right to limit, quality and safety of services or devices.

We ask that the Agency adjust the references to “service or device” to “product, service, or device.” We think the addition of the word “product” would help clarify that data may be used to ensure consumer safety and product quality across a variety of economic activities.

§ 7028(c). Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information, attempts to use a product or service after exercising the right to limit.

This paragraph is confusing. If a consumer requests a service that requires the use of sensitive personal information, the use of that personal information is already permitted by §7027(1)(1). So, there should not be a situation where a consumer requests a service that requires sensitive personal information for a purpose not covered by §7027(1). Uses of sensitive personal information required to provide a requested service are always permitted. This section should be revised to indicate the consent is required only if the business seeks to use sensitive personal information for a purpose that is not covered by §7027(1).

§ 7050(b)(2). Service Providers and Contractors. Exceptions to prohibition retaining, using, or disclosing personal information. Specific business purposes.

The use of the phrase “business purposes and services” expands the contracting requirements beyond what is found in the CPRA. The CPRA only mentions “business purposes” or “purposes” when describing how a contract should limit a service provider’s use of data. To further require the specific services to be identified creates contractual complexity without an off-setting benefit to consumers.

For example, many companies enter into “master service agreements” that generally describe how the companies will relate to their service providers and create a framework for the purchase of a variety of services – some of which may be known at the time of contracting and others which may arise in the future. Often, the addition of new services is done via quasi-contractual documents like Statements of Work, Purchase Orders, or Change Orders. These documents may, in turn, refer out to product descriptions or specifications found elsewhere.

To require all of these service descriptions to be pulled into the master agreement and enshrined at each point in the process would be very burdensome. It would also require amending contracts signed using the “purpose”-based approach adopted in the existing regulations. Statements that data may not be used except in the context of the business relationship between the parties and for the purposes of providing purchased services to the business are more than adequate to put enforceable contractual limits on service provider conduct. Providing more detail does not benefit consumers (who likely will never encounter the full master services agreement).

§ 7051 (Generally). Contract Requirements for Service Providers and Contractors.

We encourage the Agency to adopt a transition period for the execution of new contracts. The Agency’s should take note of the recent changes to the European Standard Contractual Clauses, where the European Commission acknowledged that the process of revising and updating contracts (even with very similar substantive provisions) is time-consuming and cannot be done overnight. The Agency should provide a similar transition period, where existing contracts executed in compliance with the current regulations remain valid until a certain point in time. New contracts could be expected to comply with Agency requirements a few months after they go into effect. We propose that businesses be given three months to come into compliance for new contracts, with existing contracts remaining valid for a year before changes are required.

§ 7051(e). Contract Requirements for Service Providers and Contractors. Contractual due diligence.

The Agency's statement that a business which "never enforces the terms of the contract nor exercises its rights to audit" a service provider may not claim it did not know and should not have known of a service provider's violation runs counter to the plain language of the CPRA. The CPRA clearly establishes a misconduct or gross negligence standard for a business's loss of liability protection. The Agency's proposed approach converts this standard to a mere "negligence" standard. This is not what the statute envisions. This statement should be removed.

Conclusion and contact information.

Thank you for considering our comments and recommendations. If you have any questions, you may contact Fielding Greaves at [REDACTED] or Reed Abrahamson at [REDACTED].

Sincerely,

[REDACTED]

Fielding Greaves
Sr. Director, State Government Affairs
Biocom California

[REDACTED]

Reed Abrahamson
Secretariat
International Pharmaceutical & Medical
Device Privacy Consortium (IPMPC)

From: **Tracy Locklin** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 21:00:06 (+02:00)
Attachments: National Student Clearinghouse - Comment.pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached, please find the National Student Clearinghouse's written comments submitted in response to the California Privacy Protection Agency's Notice of Proposed Rulemaking published July 8, 2022.

Thank you for your consideration.

Sincerely,

Tracy Locklin

Chief Privacy Officer

National Student Clearinghouse

Certified: CIPP/US

2300 Dulles Station Blvd., Suite 220

Herndon, VA 20171

[REDACTED] | studentclearinghouse.org

[LinkedIn](#) | [Twitter](#) | [Blog](#) | [Instagram](#)

Serving Education Since 1993

This message is proprietary to the National Student Clearinghouse, is intended only for the addressee and may contain confidential or privileged information. If you receive this message in error, please contact the sender and delete all copies.



August 23, 2022

California Privacy Protection Agency
Attention: Brian Soublet
2101 Arena Boulevard
Sacramento, California 95834

Dear Mr. Soublet:

The National Student Clearinghouse is a nonprofit organization that provides data services to the education community, including data reporting, degree and enrollment verification, electronic transcripts, and research-related services. We serve the full range of educational institutions, K-12 and higher education, nonprofit and for-profit. The Clearinghouse's voluntary data services provide over \$750 million in annual savings for institutions, and our research capabilities enable the education community to better understand student enrollment, persistence, and credential attainment.

We believe there are two places where revisions to the draft California Privacy Rights Act of 2020 (CPRA) regulations are warranted, to ensure service providers can combine data in order to serve multiple entities, and to ensure that, where nonprofit entities might be considered third parties, they are not burdened beyond what the statute intended. While we are submitting these comments on our own behalf, we believe they are likely applicable to other nonprofit entities that provide data-related services to multiple entities.

Exceptions to Prohibition on Service Providers Combining Personal Information

The CPRA amended the definition of "service provider" under the California Consumer Privacy Act (CCPA) to include a contractual prohibition on combining personal information received from, or on behalf of, a covered business with personal information received from another person or persons, or collected from its own interaction with the consumer, although service providers are permitted to perform any "business purpose" as defined by regulations promulgated under a related section of the statute.¹ Similar prohibitions are provided for in the CPRA's definition of "contractor."² In the proposed regulations no such definition of "business purpose" has been included. Instead, the general prohibition on combining personal information received from, or on behalf of, multiple covered businesses is repeated.³ And while the statute does define the term "business purpose," the definition is relatively high-level, creating ambiguity for service providers and contractors alike.⁴

¹ Cal. Civ. Code § 1798.140(ag)(1)(D).

² *Id.* at § 1798.140(j)(1)(A)(iv).

³ § 7051(a)(5) of the proposed regulations.

⁴ *See, e.g.*, Cal. Civ. Code § 1798.140(e)(5) (defining "business purpose" to include "[p]erforming services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business").



The Agency should accept the CPRA's invitation to clarify the scope of "business purposes" for which service providers and contractors may combine personal information from various covered businesses in the context of the services they provide. Such clarification is vital to commerce in our experience. Assisting the education community in understanding student pathways and achievement is predicated on our ability to combine records on a single student from multiple sources. Schools and educational organizations seek to understand student pathways and achievement so that they can improve the educational services they offer to students. Further, there is no inherent harm or risk in merging personal information from two or more sources into a single database. Rather, the potential for harm arises from what new information may be inferred about a consumer's personality traits, behaviors, or preferences from the resulting, combined personal information and the fact that the consumer (and the covered business) may have limited insight into and control over how such inferred information may be used or disclosed.

Thankfully, the Agency may take steps to permit the socially beneficial combinations described above while advancing consumer transparency and data subject rights. To that end, we recommend that the Agency incorporate into the regulations the following text as an example of a "business purpose" for which the combination of personal information from multiple sources is permitted:

"Combining personal information received from, or on behalf of, a covered business with personal information received from, or on behalf of, another person or persons, provided that: (1) the combination is authorized in contracts with each applicable covered business from which it received personal information; and (2) any new personal information regarding a consumer's personality traits, behaviors, or preferences inferred from such combined personal information is not disclosed to any person unless the consumer has provided prior written consent."

This proposed language balances the need to protect consumer's visibility into and control over the use and disclosure of their personal information with the practical realities of commerce, in which service providers and contractors are often asked by businesses to provide services that are only possible through the combination of data received from, or on behalf of, multiple sources. By focusing on the type of personal information inferred from the combination of personal information from multiple sources, the proposed language would effectively contain the harmful byproducts of such practices while also enabling service providers and contractors to realize the increased efficiencies and benefits intrinsic in merging data from multiple sources.

Obligations of Non-Profit Third Parties

The CPRA, like the CCPA that it amended, focuses on the privacy rights of consumers and the obligations of "businesses" to respect those rights and protect the privacy of the consumers they serve. The term "business" is expressly defined to exclude entities that do not operate on a for-profit basis.⁵

⁵ Cal. Civ. Code § 1798.140(d)(1).



This focus is appropriately reflected in Section 3 of the CPRA, where the purpose and intent of the CPRA is described in detail.⁶ That section contains an entire subsection on “The Responsibilities of Businesses” as well as sections on “Consumer Rights” and “Implementation of the Law,” none of which discuss the applicability of the law to non-profit entities. It is notable but not surprising that non-profit entities are not discussed in Section 3. Non-profits are not the focus of the law. While nonprofit entities may have obligations to the extent they qualify as service providers, contractors, or third parties under the CPRA, those obligations depend on their relationships with businesses.

The proposed regulations would apply several new obligations to third parties, many of which mimic the obligations placed on businesses by either the law or the proposed regulations. For third parties that are not also businesses, this would seem to go beyond the CPRA’s intended purpose to regulate for-profit entities’ collection, use, and disclosure of consumer personal information, not non-profits.

For example, both subsections (a) and (b) of proposed § 7052, related to consumer rights requests, require third parties to comply with such requests “in the same way a business is required to comply with the request.”⁷

Similarly, proposed § 7053 mandates that a business that sells or shares a consumer’s personal information with a third party must enter into a contract with the third party, which contract must require the third party to provide “the same level of privacy protection as required by businesses.”⁸

Both of these proposed regulations would extend the reach of the law beyond its stated intent and purpose, as reflected in Section 3 of the text of the CPRA. Doing so strains the text of the underlying law and could subject non-profit entities to unexpected regulatory obligations to which they have not previously been subject. We, therefore, propose that the Agency clarify that such requirements are applicable only to the extent such third parties also meet the definition of “business” under the CPRA.

Conclusion

The National Student Clearinghouse appreciates the Agency’s work in protecting the data privacy of California consumers and the opportunity to comment on the proposed CPRA regulations. If you have any questions regarding our comments, or would like to discuss these issues further, please do not hesitate to contact me at [REDACTED].

Respectfully submitted,

[REDACTED]
Tracy Locklin
Chief Privacy Officer

⁶ See text of Proposition 24, enacted by the voters of California as the CPRA, available [here](#), at p. 44.

⁷ § 7052(a)-(b) of the proposed regulations.

⁸ § 7052(a)(3) of the proposed regulations.

From: **Travis Frazier** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 21:01:30 (+02:00)
Attachments: FINAL Joint Ad Trade Letter - CPRA Regulations Comments (Aug. 23, 2022).pdf (8 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see attached for joint comments from the following trade associations: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, and the Digital Advertising Alliance. We appreciate your consideration of this letter.

Regards,

Travis Frazier

Manager, Government Relations | [ANA](#)

P: [REDACTED] | [ana.net](#) | [@ANAGovRel](#) | [LinkedIn](#)

2020 K Street, NW, Suite 660, Washington, DC 20006

The ANA drives growth for you, your brand, our industry, and humanity. Learn how at [ana.net/membership](#).



August 23, 2022

California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd.
 Sacramento, CA 95834

RE: Joint Ad Trade Comments on the Text of Proposed Regulations to Implement the California Privacy Rights Act of 2020 – CPPA Public Comment

Dear Privacy Regulations Coordinator:

On behalf of the advertising industry, we provide the following comments in response to the California Privacy Protection Agency’s (“CPPA” or “Agency”) July 8, 2022 request for public comment on the text of proposed regulations to implement the California Privacy Rights Act of 2020 (“CPRA”).¹ We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. However, we are concerned that several provisions in the proposed regulations contravene the clear text of the CPRA. We also believe that the Agency has seriously underestimated the costs that will accrue from the new, and in some cases, unclear requirements set forth in the proposed rules.² We therefore ask the CPPA to amend the proposed regulations to ensure that they align more clearly with the text of the CPRA, as described in more detail in the comments that follow below. We also ask the Agency to amend its Economic and Fiscal Impact Statement so that it more accurately reflects the significant costs that businesses will accrue from required updates to their processes and procedures to comply with new mandates under the proposed regulations.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.³ Our group has more than a decade’s worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We welcome the opportunity to engage with you in this process to develop regulations to implement the CPRA.

I. The Proposed Regulations’ “Necessary and Proportionate” Requirements Should Be Tied to Consumer Notice

The CPRA enumerates specific business purposes for which a business may use personal information *and explicitly* states personal information may be used for “other notified purposes.”⁴ The proposed regulations’ “average consumer expectation” standard would completely read out of the statute the role notice plays under the CPRA in permitting the collection and use of personal

¹ CPPA, *Notice of Proposed Rulemaking* (Jul. 8, 2022), located [here](#).

² CPPA, *Economic and Fiscal Impact Statement (STD 399)* (Jun. 28, 2022), located [here](#).

³ John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located [here](#) (hereinafter, “Deighton & Kornfeld 2021”).

⁴ Cal. Civ. Code §§ 1798.100(c), 140(e) (effective Jan. 1, 2023).

information. The proposed regulations should be modified to recognize that a business may use data as described in its privacy notices to consumers, including uses that are consistent and compatible with its disclosures.

The proposed regulations would require “[a] business’s collection, use, retention, and/or sharing” of personal information to be “reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an *average consumer would expect* when the personal information was collected.”⁵ This “average consumer expectation” standard is not the standard set forth for “necessary and proportionate” data processing requirements in the law. The CPRA itself ties its “necessary and proportionate” requirements to consumer notice, not to average consumer expectations.⁶ The law states: “A business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, *or for another disclosed purpose* that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”⁷ Similarly, the CPRA’s definition of “business purpose” is “the use of personal information for the business’s operational purposes, or other notified purposes....”⁸ The law thus clearly ties permissible data collection and use to disclosures, not average consumer expectations.

The proposed regulations substitute a new and entirely different standard in place for a clear standard set forth in the CPRA, thereby contravening statutory intent. The illustrative examples provided in proposed Section 7002 illustrate how this standard, in application, would create a result that would contravene the operational requirements of the CPRA. For example, one illustrative example would prohibit an Internet service provider from transferring any kind of geolocation information to data companies absent explicit consent from the consumer, when the text of the CPRA would permit such sales or transfers if that activity is disclosed in a consumer notice.⁹ Similarly, the illustrative examples would prohibit online retailers from using their own customers’ information to market other businesses’ products without the customer’s consent, even if a customer is made aware of that marketing data use because it is in the business’s privacy policy.¹⁰ The illustrative examples in Section 7002 contradict the consumer disclosure approach to necessary and proportionate data use taken in the CPRA. The CPPA should therefore update the proposed regulations so the requirement for “necessary and proportionate” collection, use, retention, and/or sharing is based on what is disclosed in notices to consumers rather than a malleable and fluid “average consumer expectation.”

II. The Proposed Regulations Should Follow the CPRA by Clarifying Opt-Out Preference Signals Are Optional and Should Implement Statutorily Required Safeguards to Authenticate Such Signals

The CPRA clearly states that businesses “may elect” to comply with opt out preference signals or include a clearly labeled opt-out link in the footer of their websites.¹¹ The proposed rules contradict this statutory language by stating that processing such signals is mandatory.¹² The proposed rules read

⁵ Cal. Code Regs. tit. 11, § 7002(a) (proposed).

⁶ Cal. Civ. Code § 1798.100(c) (effective Jan. 1, 2023).

⁷ *Id.* (emphasis added).

⁸ *Id.* at § 1798.140(e).

⁹ Cal. Code Regs. tit. 11, § 7002(b)(3) (proposed).

¹⁰ *Id.* at § 7002(b)(4).

¹¹ Cal. Civ. Code § 1798.135(b)(3) (effective Jan. 1, 2023).

¹² Cal. Code Regs. tit. 11, §§ 7025(b), (e) (proposed).

out of the text of the law clear language that makes opt-out preference signals optional. Instead, the proposed rules suggest that a business is mandated to honor opt out preference signals in either a “frictionless” or “non-frictionless manner,” terms that are nowhere in the text of the CPRA itself.¹³ The proposed regulations’ “frictionless” standard is extra-legal, as it is not supported by the text of the CPRA; it directly contravenes the law, which clearly makes adherence to opt out preference signals optional.

To support the proposed regulation making adherence to opt out preference signals mandatory, the Agency’s Initial Statement of Reasons (“ISOR”) for the proposed rules cites the regulatory authority given to the Agency in Section 1798.185(a)(20) of the CPRA. According to the ISOR, adherence to opt out preference signals is mandatory because the statute gives the Agency authority to issue rules to govern how a business may provide consumers with an opportunity to subsequently consent to sales or sharing of personal information. This reasoning does not describe why the Agency has gone beyond the plain text of the law by instituting a mandatory standard instead of the clear choice the CPRA envisions with respect to such signals. Moreover, it entirely ignores the fact that the regulatory directive in Section 1785.185(a)(20) itself even acknowledges that adherence to opt-out preference signals is optional. According to that section, the Agency must issue “regulations to govern how a business *that has elected* to comply with subdivision (b) of Section 1798.135,” the subdivision that describes opt-out preference signals, “responds to the opt-out preference signal.”¹⁴ By making adherence to opt-out preference signals mandatory, the Agency has ignored clear text to the contrary in the CPRA. The Agency should rewrite its opt-out preference signal regulations to reflect the CPRA’s text, which explicitly gives businesses a choice to process such signals *or* offer a clearly labeled opt-out link in the footers of their websites.

Additionally, the Agency’s proposed opt-out preference signal rules fail to implement key provisions of the CPRA that set guardrails around the development of the optional opt-out preference signals. The CPRA specifically tasks the Agency with “issuing regulations to define the requirements and technical specifications for an opt-out preference signal,” which would ensure the signal: (1) cannot unfairly disadvantage certain businesses in the ecosystem, (2) is clearly described; (3) clearly represents a consumer’s intent and is free of defaults presupposing such intent; (4) does not conflict with commonly-used privacy settings consumers may employ; (5) provides a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) provides granular opt-out options for consumers. Not one of these key safeguards—which are explicitly in the text of the CPRA and which the Agency is instructed to effectuate via regulations—is addressed in the proposed rules.

As written, the proposed regulations would create widespread confusion because they do not clarify how opt-out preference signals can meet the safeguards requirements that are set forth in law. The proposed regulations also do not call for any standardization for opt-out preference signals. The Agency should create a process to address the requirements for opt-out preference signals that reflects the CPRA’s stated safeguards, rather than make businesses guess which signals comply with the law’s mandates as well as how companies should address conflicting signals with respect to a single individual. Regulations furthering the CPRA’s opt-out preference signal safeguards are necessary to ensure businesses can verify that the signal, or the “mechanism” or “tool” that provides the signal, has complied with the various requirements under the CPRA, including requirements related to presentation of choices, default settings, disadvantages to businesses, and reflection of consumer intent. The Agency should address these statutory requirements concerning mechanisms that set opt-out preference signals before adopting regulations concerning honoring such signals. Guidance is first

¹³ *Id.* at § 7025(e).

¹⁴ Cal. Civ. Code § 1798.185(a)(20) (effective Jan. 1, 2023) (emphasis added).

required to govern the mechanisms used to set signals to ensure such tools are offered in compliance with law and so that businesses receiving such signals can be assured that the signals are legally set preferences.

III. Section 7050(c) is Duplicative of the CPRA and Should Be Removed From the Proposed Regulations

Section 7050(c) of the proposed regulations merely restates the CPRA. The section should therefore be removed from the proposed regulations because it provides no additional context or clarity that is not already in the text of the law. The proposed regulation reaffirms the CPRA’s text, which prohibits companies from offering cross-context behavioral advertising services to businesses while occupying the “service provider” role.¹⁵ Section 7050(c) of the proposed regulations simply restates the law, which plainly permits entities to provide advertising and marketing services to businesses as “service providers,” and even permits them to combine personal information for advertising and marketing purposes in some circumstances so long they do not “combine the personal information of opted-out consumers that the service provider... receives from, or on behalf of, the business with personal information that the service provider receives from, or on behalf of, another person or persons or collects from its own interactions with consumers.”¹⁶ The text used in Section 7050(c) of the proposed regulations is virtually identical to the text of the CPRA on this point, and it is also duplicative of the section immediately preceding it, Section 7050(b)(4). Because the proposed regulation restates the CPRA provision explaining that an entity may provide advertising and marketing services as a service provider, but may not engage in cross-context behavioral advertising (the targeting of advertisements to consumers based on personal information combined from multiple businesses),¹⁷ Section 7050(c) adds no additional clarity to the CPRA and should thus be removed from the proposed regulations.

IV. The Proposed Regulations Should Clarify a Third Party’s Provision of Information About its Business Practices to a First Party Satisfies the Third Party’s “Notice at Collection” Obligations

The proposed regulations place “notice at collection” requirements on entities that “control the collection” of personal information.¹⁸ These entities may include first party entities, which, for example, own the websites that consumers may visit, as well as third party entities that may control collection of personal information about a consumer when he or she visits a first party’s website. Section 7012(g)(1) states the first party “as well as the third party controlling the collection of personal information, shall provide a notice at collection.”¹⁹ The proposed regulations state that a first party’s “notice at collection” must include “the names of all the third parties that the first party allows to collect personal information from the consumer.”²⁰ Alternatively, the proposed regulations permit “a business, acting as a third party and controlling the collection of personal information, [to] provide the first party [with] information about its business practices for the first party to include in the first party’s notice at collection.”²¹ Although the proposed regulations provide this option to third parties, they do not clarify that a third party’s provision of information about its business practices to a first party will satisfy the third party’s “notice at collection” obligations. The Agency should consequently add a sentence to Section 7012(g)(2) of the proposed regulations to clarify that a third party that provides

¹⁵ *Id.* at § 1798.140(e)(6).

¹⁶ *Id.*

¹⁷ *Id.* at § 1798.140(k).

¹⁸ Cal. Code Regs. tit. 11, § 7012(g)(1) (proposed).

¹⁹ *Id.*

²⁰ *Id.* at § 7012(g)(2).

²¹ *Id.*

information about its business practices to a first party for inclusion in that first party's notice at collection has satisfied the third party's own "notice at collection" obligations.

V. The Proposed Regulations Should Permit Businesses to Leverage Existing In-Market Icons and Choice Mechanisms

According to the CPRA, businesses may offer an "alternative opt-out link" to "provid[e] consumers with a single, clearly-labeled link that enables consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate 'Do Not Sell or Share My Personal Information' and 'Limit the Use of My Sensitive Personal Information' links."²² The proposed rules would require the title for that link to be "Your Privacy Choices" or "Your California Privacy Choices," and would require it to direct a consumer to a webpage that enables them to make choices to opt out of sales, opt out of sharing, and limit the use and disclosure of sensitive personal information.²³ For entities that use such an "alternative opt-out link," the proposed regulations would require them to also include the following graphic next to the link:



The proposed graphic icon is confusing. Its inclusion of just one check mark and one "x" suggests just *one choice* will be made via the alternative opt-out link, when in reality the link would provide consumers the ability to make three choices: (1) the choice to opt out of personal information sales; (2) the choice to opt out of personal information sharing; and (3) the choice to limit the use and disclosure of sensitive personal information. The CPPA should remove the prescriptive opt-out icon requirement and instead allow the marketplace to continue to leverage existing, widely deployed iconography provided the mandatory language is present.²⁴

VI. The Proposed Regulations Should Not Require Opt-Out Requests to Be Sent Downstream

The proposed regulations would require businesses to send opt-out requests to other parties to which the business transferred related personal information.²⁵ This requirement is not reflected in the CPRA and would not further consumer choice. The CPRA empowers consumers to express choices to businesses individually via a clearly labeled opt-out link, and pursuant to the text of the CPRA, those choices are effective against those businesses alone. A rule requiring businesses to send opt-out requests to other downstream entities actually removes choices from consumers by eliminating their ability to make choices effective against certain businesses while still enjoying the benefit of data use by other companies. Additionally, the requirement to forward opt-out requests to other parties is not present in the text of the CPRA. The CPRA clearly requires businesses to send *deletion* requests to contractors, service providers, and third parties, but the text does not include the same requirements for opt-out requests.²⁶ The existence of the requirement to forward deletion requests to other parties while the same requirement is absent for opt-out requests shows that the CPRA does not intend to impose an opt-out flow down requirement on businesses. The requirement for businesses to transmit opt-out requests to other parties should be removed from the proposed regulations.

²² *Id.* at § 7015(a).

²³ *Id.* at §§ 7015(b) & (c).

²⁴ Digital Advertising Alliance, *YourAdChoices*, located [here](#).

²⁵ Cal. Code Regs. tit. 11, §§ 7026(f)(2) & (3) (proposed).

²⁶ Cal. Civ. Code § 1798.105(c)(1) (effective Jan. 1, 2023).

VII. The Agency Should Delay Enforcement for One Year Following Finalization of the Proposed Regulations

According to the CPRA, the Agency is required to finalize the regulations implementing the law by July 1, 2022.²⁷ This date has unfortunately already passed, and the regulations implementing the CPRA are not yet final. If the proposed regulations were made final by the statutorily mandated date of July 1, 2022, businesses would have had a full year to come into compliance with the regulations' terms prior to facing enforcement actions from the CPPA, which may commence on July 1, 2023.²⁸ In alignment with the CPRA timeline, the Agency should delay enforcement actions for one year following the finalization of the regulations implementing the law. Such an enforcement forbearance would sync with the clear language of the CPRA, which was structured to give businesses a full year to modify their practices, as needed, to comply with regulatory requirements before they could be penalized for violating those obligations.

VIII. The Data-Driven and Ad-Supported Online Ecosystem Benefits California Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent study found that the Internet economy's contribution to the United States' GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.²⁹ In 2020 alone, it contributed \$2.45 trillion to the U.S.'s \$21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of \$300 billion.³⁰ Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.³¹ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.³² The same study found that the ad-supported Internet supported 1,096,407 full-time jobs across California, more than double the number of Internet-driven jobs from 2016.³³

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulations that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.³⁴ One recent study found that “[t]he U.S. open web’s independent publishers and companies reliant on open web tech would lose between \$32 and \$39 billion in annual revenue by 2025” if third-party tracking were to end “without mitigation.”³⁵ That same study found that the lost revenue would become absorbed by “walled gardens,” or entrenched market players, thereby consolidating power and revenue in a small group of

²⁷ *Id.* at § 1798.185(d).

²⁸ *Id.*

²⁹ Deighton & Kornfeld 2021 at 5.

³⁰ *Id.*

³¹ *Id.*

³² *Id.* at 6. See also Digital Advertising Alliance, *Summit Snapshot: Data Drives Small-and Mid-sized Business Online, It's Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located [here](#).

³³ Compare Deighton & Kornfeld 2021. at 121-123 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,096,407 jobs in 2020).

³⁴ See John Deighton, *The Socioeconomic Impact of Internet Tracking 4* (Feb. 2020), located [here](#) (hereinafter, “Deighton 2020”)

³⁵ *Id.* at 34.

powerful entities.³⁶ Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated \$15.5 billion in revenue.³⁷ Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Californians' Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,³⁸ and decreased digital advertising budgets directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.³⁹ And, consumers tell us that. In fact, consumer valued the benefit they receive from digital advertising-subsidized online content at \$1,404 per year in 2020—a 17% increase from 2016.⁴⁰ Regulatory frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such regulatory frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.⁴¹ Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.⁴² Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁴³

³⁶ *Id.* at 15-16. See also Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*, EUROPEAN COMPETITION JOURNAL (Dec, 18, 2020), located [here](#).

³⁷ Deighton 2020 at 28.

³⁸ See Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located [here](#).

³⁹ See John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located [here](#).

⁴⁰ Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

⁴¹ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located [here](#).

⁴² Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located [here](#).

⁴³ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located [here](#).

IX. Conclusion

During challenging societal and economic times such as those we are currently experiencing, laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider the proposed regulations' potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy as you continue to refine the draft rules.

* * *

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
[REDACTED]

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
[REDACTED]

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP